Opportunities for U.S.-China Scientific Collaboration in Building a Bilateral Quantum Network

by

Nolan R. Hedglin

B.S. Mathematics, B.S. Physics,
United States Military Academy (2018)

Submitted to the Department of Electrical Engineering and Computer Science
and
Institute for Data, Systems, and Society

in partial fulfillment of the requirements for the degrees of

Master of Science in Electrical Engineering and Computer Science
and
Master of Science in Technology and Policy

at the
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2020

© Massachusetts Institute of Technology 2020. All rights reserved.

Author_____
Electrical Engineering and Computer Science
and
Technology and Policy Program
July 29, 2020

Certified by_____
Isaac L. Chuang
Professor of Physics
Professor of Electrical Engineering and Computer Science
Thesis Supervisor

Accepted by_____
Leslie A. Kolodziejski
Professor of Electrical Engineering and Computer Science
Chair, Department Committee on Graduate Students

Accepted by_____
Noelle E. Selin
Director, Technology and Policy Program
Associate Professor, Institute for Data, Systems, and Society and
Department of Earth, Atmospheric and Planetary Sciences

Opportunities for U.S.-China Scientific Collaboration in Building a Bilateral Quantum Network

by

Nolan R. Hedglin

Submitted to the Department of Electrical Engineering and Computer Science
and
Institute for Data, Systems, and Society

on July 29, 2020, in partial fulfillment of the
requirements for the degrees of

Master of Science in Electrical Engineering and Computer Science
and
Master of Science in Technology and Policy

Abstract

From advancements in time transfer to networked science, quantum networks can enable a new host of experiments that would not otherwise be achievable. We can learn a lot about building such a network to connect quantum resources globally through international cooperation. Toward this end, we argue that the countries best equipped to forge the path for building a global quantum network are the two largest countries spearheading research in the field: the U.S. and China. An analysis of each country's innovation landscape tells us that their primary interest in quantum technology is motivated by the desire to modernize their military. Both countries may be apprehensive to collaborate because the perceived security risks of a knowledge exchange far outweigh the benefits they would receive in accelerating innovation. Any proposal for a joint project is mired in the urgent geopolitical crisis that is U.S.-China relations. As escalatory retaliation, the U.S. has adopted a policy of innovation isolationism since 2019 in an effort to minimize scientific and technological exchanges between the two countries. We argue that the U.S. security framework needs a paradigm shift because the country cannot address several major vulnerabilities in its current security posture without building bilateral stability with China. To support this claim, we describe how a lack of bilateral stability could create unnecessary escalation in cyberspace and hinder each country's ability to solve global security issues such as climate change. Drawing upon the historical analogy of U.S.-U.S.S.R. cooperation in space exploration during the Cold War, we propose a framework for a joint quantum project that can achieve U.S. scientific and diplomatic goals alike. Finally, we present experimental work being done at MIT Lincoln Laboratory to better understand some of the technical challenges associated with building a bilateral quantum link.

Thesis Supervisor: Isaac L. Chuang
Title: Professor of Physics
Professor of Electrical Engineering and Computer Science

Acknowledgments

I would like to thank the following people who have been a tremendous help in writing this thesis: my on-campus advisor, Isaac Chuang, who has taught me the value of being more cerebral and deliberate with my rhetoric. Ike's ideas and feedback were pivotal to the success of this thesis; my Lincoln advisor and scuba diving connoisseur, Matthew Grein, who has supported my work in and out of the laboratory every single day, in addition to giving me the occasional ride to work. I would be hard-pressed to name a more selfless individual who truly cares about a person's well-being and success; Scott Hamilton, who is one of the best leaders and communicators I have ever had the privilege of knowing. Scott epitomizes what it means to be a steward of one's profession. He is a role model for young researchers everywhere; Catherine Lee and Eric Bersin, who have provided top-notch advice on nearly every single topic floating around in my brain. To each of you: it would be impossible to fully express my gratitude for your wit, your humor, your perspective, your car, and your beer expertise; Ben Dixon, who is possibly the oldest Millenial I know. Ben is someone I look up to both literally and figuratively; Ryan Murphy, Matlab extraordinaire and devout family man. Ryan's kindness and willingness to help me debug knows no bounds; everyone else in or from Group 67 who has helped me along the way, such as Jennifer Wang, Jessica Chang, Katia Shtyrkova, Claudia Fennelly, Mark Stevens, Terri Welch, Alicia Baldi; and The Group 89 and MIT Quanta members who have provided advice on numerous occasions: Colin Bruzewicz, Robert McConnell, Jules Stewart, John Chiaverini, Jeremy Sage, Jules Stuart, Jasmine Sinanan-Singh, Curtis Northcutt, and everyone else who I have forgotten to mention.

Finally, I would like to thank my family and everyone — from leadership down to the students — in the Technology and Policy Program who have made these last two years something truly special. To Frank Field and Noelle Selin, the good-cop/bad-cop I never knew I needed in my life. Our program mom, Barbara DeLaBarre, who moonlights as a singer in the Washington, D.C. underground karaoke scene. Ed Ballo, who inspires me to continue pursuing my hobbies and setting aside time to appreciate the finer things in life. My roommates — Hannah Whisnant, Becca Browder, and Tomas Green — who have been and I anticipate will continue to be an invaluable source of joy in my life. And every single student in TPP: I cannot fathom my grad school experience without you.

THIS PAGE INTENTIONALLY LEFT BLANK

Contents

THIS PAGE INTENTIONALLY LEFT BLANK

List of Figures

THIS PAGE INTENTIONALLY LEFT BLANK

List of Tables

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 1

Introduction: the Disruptive Innovation of a Quantum Network

The ability to process and transfer information in new ways can be a driving force for innovation. Subsequently, thinking about information as quantum can enable a new host of applications that would not otherwise be achievable. On the processing side, quantum computers have been touted for their ability to leverage the principles of quantum mechanics to simulate computationally-intractable molecular systems and break asymmetric encryption by solving the discrete logarithm problem efficiently [Sho97]. But equally as exciting is the ability to transport quantum information between locations, known as quantum communications (used interchangeably with "quantum networking" throughout).

The purpose of this thesis is to analyze the field of quantum networking through the lens of contemporary U.S.-China relations (Chapters 2 and 3) and weigh the security risks of establishing a joint quantum project between the U.S. and China (Chapter 4). Before we can discuss policy, however, we need to understand what quantum networking is. This chapter is not intended to be a scientifically comprehensive analysis of quantum networking research. Rather, it is a qualitative grounding meant to inform our policy discussions in Chapter 2, 3, and 4.

In Sections 1.1 and 1.2, we discuss how quantum networking will be a *disruptive innovation* — defined as innovation that changes how an existing market functions [CB95] — in the coming

decades by illustrating applications of a quantum network that could supplant existing classical methods. Then, in Section 1.3 we explore some of the design challenges associated with scaling up a quantum network, concluding that international cooperation is required for turning it into a global-spanning technology.

1.1 Differentiating classical from quantum information

First, in order to understand a quantum network and how it differs from a classical network, we need to understand the type of information it supports. The scope of this analysis will be limited to the properties of quantum information that are most relevant to the engineering challenges discussed in Section 1.3 and will be less comprehensive than what has been presented elsewhere [NC10]. The fundamental building block of quantum information is a two-state quantum system called the qubit, which has some of the following properties [NC10]:

- *Superposition* - undisturbed, a quantum system is able to exist in multiple states at once. This means that a qubit can exist as a linear combination of 0 and 1 before measurement;
- *Entanglement* - a pair of qubits are considered entangled when the state of each qubit in the pair cannot be described independently of the state of the other;
- *Measurement* - observing a qubit will yield a specific value with some prior probability, but will cause a collapse in the qubit's wave function; and
- *Decoherence* - when a qubit interacts with the environment, it can irrecoverably leak information about its state, making the qubit unusable.

1.2 Applications enabled by the emergence of quantum networking

The power of any network is correlated with the applications it can enable. This notion will become important when trying to understand what makes a quantum network such a promising prospect for the future of information sharing. First and foremost, a quantum network will be important because of its ability to facilitate communication between two quantum computers in their native language of qubits, which no other network can do today. Beyond that, quantum networks can also be used to improve upon existing applications that use classical networks as the backbone for operation. The example that has garnered the

most attention is using a quantum network to distribute encrypted keys between digital hosts. In this section, we discuss quantum key distribution and consider three other applications — time transfer, networked science, and distributed quantum computing — where quantum networking could have a clear practical advantage over its classical counterpart.

1.2.1 Secure communication

Symmetric encryption has been traced back to as early as the fifth century B.C.E., when the Spartan's invented the first transposition cipher known as the *scytale* [Sino0]. With the invention of the computer, we drastically increased the rate at which we could encrypt messages. In addition to the symmetric forms of encryption that were common before the Internet, we now have methods for securing a communication channel between two individuals who do not already share a secret key but have authenticated themselves to one another — known as asymmetric encryption — by leveraging aspects of computational complexity in order to provide security. Today, information transported over the Internet is largely secured by the practice of using asymmetric encryption to get two individuals to agree on a shared secret key they can use for future communications; this is known as a key exchange. The most common forms of key exchange today use either RSA [RSA78] or Diffie-Hellman [Mer78; DH76] protocols, which assume that an eavesdropper cannot quickly solve the discrete logarithm problem and thus learn the shared secret key. In 1997, Peter Shor developed a quantum computing algorithm that broke this security assumption [Sho97]. Quantum key distribution (QKD) was proposed as a solution to key exchange that does not rely on the hardness of the discrete logarithm problem.

The power of using quantum information to distribute secret keys is that the presence of an eavesdropper can be detected with a probability of $\mathrm{P}(\text{detect}) = 1-2^{-p}$ for every p bits Alice and Bob disclose. The *no-cloning* theorem states that it is impossible for an eavesdropper to create an independent and identical copy of an unknown quantum state. Therefore, eavesdropping would require measurement of the quantum information being exchanged, which will disturb the original state of the qubit. Two protocols that exist for QKD are: BB84 [BB14], which involves using any qubit basis Alice wishes to transmit information; E91 [Eke91], which uses pairs of entangled photons for detecting eavesdropping. However, QKD is not without its faults. The BB84 and E91 protocols do not provide authentication, which means a classical authentication algorithm will still need to be used in order to provide complete security.

Additionally, research into lattice-based encryption protocols — which offer a way of doing key exchange and authentication that is resistant to being attacked by a quantum computer — has matured in recent years, meaning that QKD no longer has a clear advantage over any classical counterpart [NCS20].

1.2.2 Position, navigation, and timing

Time and position information are continuous variables whose precision can be improved by advancements in frequency transfer. The goal of frequency transfer is to get separate clocks — each of which behave as an oscillator — to come to an agreement over their oscillatory frequency and offset. Using the network to achieve this is known as *syntonization* and *synchronization*, respectively; they are the core components of time transfer. The precision with which we can transfer time is then limited by our ability to match clock frequency and offset. Today, the most common form of time transfer, Global Positioning System (GPS), achieves nanosecond-level stability by using a network of satellites in low Earth orbit (LEO) and ground stations as the platform for atomic clocks to communicate.

Coupled with sensors, position and timing is used to achieve a better understanding of our environment. For the military, this could mean gathering information about the terrain within which units operate. For climate scientists, it could mean tracking global weather patterns, carbon emission levels, or even fluctuations in the Earth's gravitational field [Tap+05]. These applications of domain awareness allow us to make more informed decisions by enabling a better understanding of the world around us and its resources. But global time transfer is important to more than just determining the location of an object or the characteristics of its environment. In addition to domain awareness, time transfer is also important for event coordination. It is used in database management [Cor+13] and tracking activity in financial markets [Lom+16]. Chronicling online activity would be an impossible task without the ability to track and record highly precise time stamps.

We can achieve significantly better performance than off-the-shelf GPS in time transfer by treating clock signals as quantum. As depicted in Figure 1-1, the stability offered by GPS pales in comparison to commercially available and state-of-the-art laboratory clocks, thus barring a number of scientific applications requiring precise metrology. Instead, we can achieve higher levels of stability by transferring individual qubits containing the clock signal or by distributing entanglement between each node in a clock network [Chu00; Joz+00]. It has been proven that

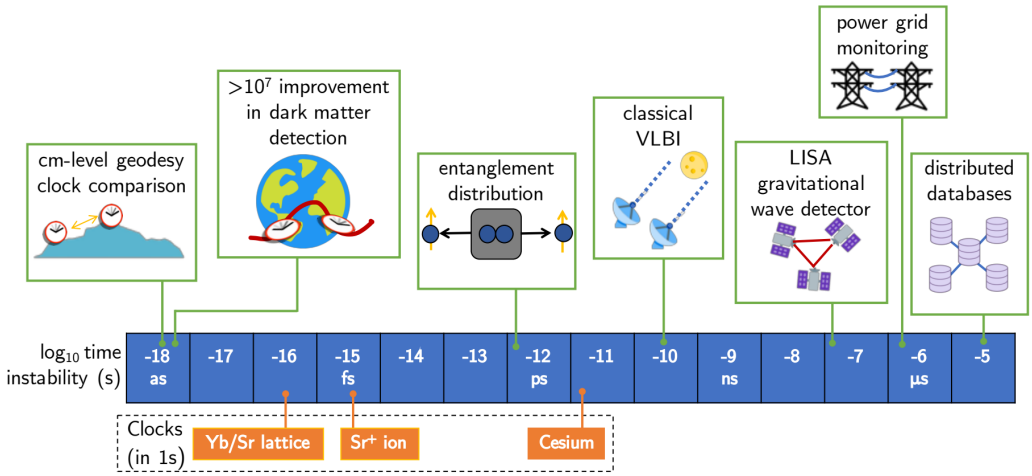

Figure 1-1: Potential applications enabled by achieving certain levels of time transfer stability. The most widely used time transfer technique (GPS) can achieve 10^{-9} s fractional frequency stability, which measures the normalized difference between the actual frequency of the clock network and the nominal frequency. Off-the-shelf clocks can easily reach 10^{-11} s (cesium clocks) and 10^{-13} s (hydrogen masers) levels of stability. This illustration was made by Helena Zhang. [Zha19]

quantum clock synchronization through entanglement can achieve Heisenberg-limited scaling in stability, which is defined as the optimal rate at which the accuracy of a measurement scales with its required energy. This means we could potentially see stability in the 10^{-17} s range [Zha19], matching state-of-the-art laboratory clocks [Kóm+14; Blo+14].

1.2.3 Networked astrophysics

Networked astrophysics is one application in particular that can be seen as a matrimony between event coordination and domain awareness. Prior to the introduction of computer networks, telescopes would collect information about interstellar light and process it locally. Networks, however, enable us to cleverly construct arrays of telescopes that improve our ability to determine the angular resolution of photons being detected. This technique, known as very-long-baseline interferometry (VLBI) in radio astronomy, was used to image the event horizon of the M87 singularity [Doe09]. Astrophysics is one example where using networks enhances our ability to conduct scientific experiments, but it is an important example because it dispels the notion that networks are only useful as a tool to help scientists communicate results; a

network *itself* can be used as the tool for discovery.

Performance of telescope arrays is limited by the maximum possible distance that an array of telescopes can be connected, known as the *baseline*. In the visible and infrared ranges, this is limited to a few hundred meters using classical interferometric techniques because of photon loss and phase fluctuations [GJC12]. In 2012, Gottesman et al. proposed a protocol for extending the baseline to arbitrary lengths by distributing entanglement between telescopes [GJC12]. One downside of the protocol, however, is that it requires entanglement distribution rates equal to the photon detection rates of the telescope array, which were thought to be out of reach using today's technology. However, in 2019 Khabiboulline et al. significantly reduced the rate requirements by encoding and compressing the stellar information in a way that still allowed retrieval of the original quantum state [Kha+19a; Kha+19b], thus re-introducing the feasibility of telescope arrays connected by a single quantum network. If we can connect arrays of telescopes to a quantum network, then our ability to resolve stellar activity could improve dramatically.

1.2.4 Distributed quantum computing

A quantum network can be used to connect multiple smaller quantum computers together to form one cluster [Kim08]. The benefit of doing this over using a classical network for connecting quantum computers because its phase space — the space in which all possible quantum states are represented — grows faster as the network scales. Suppose we have k nodes in a network, each with n logical qubits. When fully connected in a classical manner, the phase space of the system is $k2^n$ because there are k independent nodes. If we connected the nodes using a quantum channel, however, we expand the phase space to 2^{kn} because the entire network can be treated as a single quantum computer with kn logical qubits. When perfectly connected, distributed quantum computing can become an additional solution to scaling the quantum processing units being developed by companies Google [Aru+19], IBM [IBM20], and Rigetti [Cal+18].

1.3 What makes building a quantum network challenging

If we want to build a versatile network for sharing quantum information across multiple nodes, we will need to reliably distribute entanglement [Kim08; WEH18] — be it through photons

or particles. Unfortunately, existing network infrastructure is not configured in such a way that it can support the distribution of entangled pairs immediately. For example, suppose we want to share entangled photons. As illustrated by the following three engineering challenges, there are significant restrictions on how we can achieve even this fundamental requirement. Furthermore, design solutions to existing problems often beget more problems.

1.3.1 Sensitivity to the outside environment

One of the most important properties of a network is its reliability. Communication is a daily part of our lives and if a network is too fragile or error-prone to support continual operation, then its benefit will be severely limited. Computer networks circumvent the issue of fragility by adding redundancies and error correction. As a result, classical packets of information do not need to be completely isolated from the external environment because changes to the signal are less likely to affect the content being shared.

A quantum network needs some isolation from the environment in order to be operational (i.e. qubits need to maintain coherence). This does not imply that the entire network needs to be sealed off in a vacuum, but it does give an indication as to how challenging it is to adapt small scale experimental results into large spanning networks. Because decoherence is an irreversible process, we cannot observe qubits, store it, and recreate the quantum state at a later time [Pre98].

In addition to implementing quantum error correction techniques [Ben+96], one solution to this problem is by continually creating entangled pairs to be distributed between nodes and used immediately as quantum information is processed. By employing this design, however, we limit the rate of quantum information transfer across a network to the rate at which we successfully distribute entanglement, which means entanglement pair generation rate and photon loss now becomes a concern.

1.3.2 Distance limitations

Nodes separated by a greater distance will experience more loss than those close to one another. When faced with the challenge of power loss across a channel, early network engineers came up with the idea of observing the signal at an earlier stage in the channel and re-transmitting a copy of the original signal at an increased power. This was first done electrically with a

repeater, then optically with an amplifier.

Such a technology would be a welcome solution to overcome distance issues in a quantum networks, especially since minimizing link loss is of paramount importance. Unfortunately, the no-cloning theorem prevents us from making an exact replica of this technology. Observing the signal for the purpose of re-transmitting it would disrupt the state.

One proposed solution is the use of a quantum repeater [Mun+15]. Quantum repeater design is an active area of research and one promising scheme employs entanglement distribution and swapping [Hal+07]. Entanglement swapping is the process of transferring entanglement between two pairs of entangled photons, each located at a different node. By performing a Bell-state measurement [Bel64] between one signal photon from each entangled pair at a central location, the two photons held at each node become entangled. In order to maximize the fidelity of the entanglement swap, pairs must be indistinguishable from one another in every way except for the basis (e.g. their polarization or timing arrival) in which we choose to measure them [Lee+18]. This includes temporally, which means the arrival time of entangled photons at their intended destination must be known to a higher level of precision than that of the pulse width.

1.3.3 Network synchronization requirements

For a successful entanglement swap between two nodes, time synchronization in a quantum network requires the temporal overlap of two laser pulses at their respective detectors [Lee+18]. If the pulses are both 1 ps in width, then this means their *relative* arrivals must be synchronized to a fraction of 1 ps. This is challenging, but achievable, between two network nodes. However, synchronization is more complicated when scaling the network to multiple nodes. A multi-node network requires synchronizing the relative arrivals for many pairs of entangled photons, which is a task that may end up requiring precise time transfer across the entire network.

1.4 Conclusion: a global quantum network requires close international cooperation

In addition to the challenges presented in Section 1.3, there are still many other political and technical questions that will need to be addressed. Re-configuring existing networking infrastructure to support the transport of quantum information will likely be a monumental undertaking, and it is unclear if existing fiber infrastructure will even be useful for the global transport of quantum information.

The Internet largely "exists" in large servers connected by underwater cables that span across oceans [Sat19], but in order to use them for quantum networking it could likely require placing a string of quantum repeaters along the ocean floor. Quantum repeater technology is still in its infancy, and it may never reach the point where it is robust enough to withstand the environmental fluctuations of the ocean floor. Because of the maturity of free-space optical links in near and low Earth orbit [Bor+09], it seems reasonable to assume that a near-term long-distance quantum network would also utilize free-space links. This subsequently raises several more questions about how to manage network boundaries between countries that wish to control information flow within their jurisdiction, which has become commonplace for the Internet [Pag19]. This represents merely another issue that has yet to be fully resolved.

1.5 The structure for the rest of this thesis

The overarching goal of this thesis is to explore quantum networking collaboration between the U.S. and China, who are the two largest countries spearheading research in quantum information, within the context of current U.S.-China relations. In order to do so, we must first identify each country's reasons for pursuing quantum technology — not merely the network that connects quantum devices — and their stance on its development as a tool for diplomacy. In Chapter 2, we address these questions by looking at the stakeholder landscape for quantum technology and identifying what drives technology development in each country. At first glance, hopes for cooperation appear bleak under the prevailing security posture the U.S. has chosen to adopt. So, in Chapter 3, we propose a new security framework for improving relations with China and apply it to the world of quantum communications research. In Chapter 4, we outline a framework for a establishing a bilateral quantum link between the

two countries. Finally, in Chapter 5, we present experimental results for understanding some of the technical challenges associated with a joint quantum project.

Chapter 2

Innovation Models and Stakeholder Power Dynamics for Quantum Technology

Innovation does not happen in a political vacuum. A technology's development and integration into daily life are influenced heavily by its stakeholders' expectations and values. This consideration is important in predicting how global-spanning technologies such as a quantum network may develop. In order to coordinate quantum networking seamlessly between countries — or, to a lesser extent, identify opportunities for cooperation — we need to have an idea of the political environment within which a country innovates.

One way to illustrate this environment is by identifying stakeholders, delineating their expectations, and defining their relationships with one another [NR18]. Understanding the interplay between stakeholders in the U.S. and China is pivotal for identifying points of conflict within both countries regarding the access and control of quantum technology. When aggregated, this information can be used to broadly define each country's goals for deploying quantum technology, which will prove useful when developing plans for mitigating technology-driven conflicts as well as accelerating innovation through cooperation.[1]

[1]The stakeholder framework I create may also be useful in formulating policy solutions regarding the usage of quantum technology domestically, but this portion of analysis is not as pertinent to the task of identifying

First, we address some overarching factors that affect stakeholder motivations in Section 2.1. Then, in Section 2.2, we create a new framework for understanding technology development through a political lens. In Sections 2.3 and 2.4, we apply our framework to quantum technology research in the U.S. and China.

2.1 Considerations in assessing stakeholder motivations

In this section, we briefly discuss two aspects of technology governance that will influence how the U.S. government and the Communist Party of China (CCP or the Party) choose to treat an emerging technology such as quantum information science. It would be convenient to answer all questions about government investment in quantum technologies through the lens of political ideology. By doing so, however, we run the risk of treating an entire stakeholder group's belief system as monolithic and static in the presence of new information. Additionally, there is the added danger that a stakeholder uses "ideology" as a mask for selfish intentions.

Alternatively, we could focus our analysis to a more granular level by using the lens of individual stakeholder circumstance (e.g. the state of national security, the net worth of a company, an individual's income, etc.) to answer the same questions, but by doing so we may fail to account for important societal norms. In illustrating the stakeholder triangle we create in Section 2.2, we must tread the line between these two extreme lenses carefully by broadly identifying subgroups within each country who have similar motivations and access to information.

2.1.1 How problems in access and control are resolved

A new technology can exacerbate the tension in a relationship by shifting the balance of power between two stakeholders [Fio16]. Subsequently, those involved must come to an agreement on managing its access and control. This solution can take the form of a technical restriction, a policy, or some combination thereof. For instance, if the U.S. government is concerned about criminals using quantum computers to break its citizens' encrypted messages, this risk can be mitigated by proposing that every messaging service move to quantum-resistant algorithms. If this technical solution proves too challenging to implement in the near term, then a stop-gap policy solution could be amending the Computer Fraud and Abuse Act (18 U.S.C. § 1030) to criminalize encryption cracking.

opportunities for international collaboration.

When a technology is particularly disruptive, the process for coming to an agreement could potentially be messy and never fully resolved. For example, encryption software first became widely accessible to the public in 1991 with Pretty Good Privacy [Zim96]. Consequently, a decade-long legal battle transpired between the government and the public over whether encryption software should be classified as a weapon and thus subject to International Traffic in Arms Regulations (ITAR) [Sino0]. The government vehemently opposed the distribution of encryption software to the public because it made the job of law enforcement much more challenging [Vol18]. After the courts sided with the public, the government did not stop there, pursuing other tactics to weaken the public's access to encryption software — including controlling the development of cryptographic standards on the Internet so the NSA could implant a backdoor [PS18], as well as proposing federal legislation to revoke content moderation protections provided by the Communications Decency Act (47 U.S.C. § 230) for technology firms who do not mandate a backdoor on their end-to-end encrypted messaging services [Rob20].

2.1.2 Techno-optimism versus techno-pessimism

It is also worth considering to what extent a country's government views technology as an opportunity to augment or a threat to weaken their power. This will help in identifying places where the U.S. and China can cooperate in quantum networking because the effort will likely be spearheaded by a mélange of public officials and technologists.

Long-standing approaches to governance will affect how a government treats emerging technologies. The CCP takes a more top-down approach to solving societal problems, which helps them retain more control over the direction of the country [Lor13]. This is in contrast to the bottom-up federalist approach of solving problems in the United States [Toc40] where, according to Justice Louis Brandeis in 1932, states are afforded the chance to act as a "laboratory" for democracy (285 U.S. 262). For example, a sufficiently large quantum computer would be a powerful tool for monitoring the flow of information between individuals using an end-to-end encrypted messaging app that implements a Diffie-Hellman key exchange to generate shared keys. This aspect of its development would be more enticing to a government exercising top-down governance because it could enable more control over complex social systems.

A government's techno-optimism also depends on its makeup. During Mao Zedong's rule, military science rose to prominence in China because national defense became a top priority

for the Party [LX95]. As a result, scientists and engineers saw an increase in social status during these years [Gre05]. This subsequently contributed to a rise in the proportion of science, technology, engineering and mathematics (STEM) graduates that are Party officials. In 2003, the number of provincial leaders who came from a STEM background was estimated at 1 in 3 [Li03], far greater than the roughly 1 in 15 U.S. Congresspeople with a STEM background as of 2018 [Man18]. Although it appears the proportion of Party officials with a STEM background is decreasing [Zho17], the Party's interest in finding technology-focused solutions to problems in governance remains, as evidenced by the development of the Great Firewall [Moz15].

2.2 The stakeholder triangle

In this section, we use a diagrammatic representation of the stakeholders involved in the quantum technology innovation landscape in order to better understand its development through a political lens. Depicted in Figure 2-1, we create a stakeholder triangle framework — which is broadly applicable to any emerging technology — that contains three main groups: the *government*, which includes the military and other federal agencies; *technologists*, which includes anybody who helps develop quantum tech; and the *public*, which includes anyone who wants access to quantum technology, such as researchers and financial firms, but do not have a direct hand in its development.

Each stakeholder has something to offer in the development of quantum technology and expects something in return. We discuss the government-public, technologist-public, and government-technologist relationships in Sections 2.2.1, 2.2.2, and 2.2.3, respectively. We note that stakeholders are not monolithic in their desires and expectations. For instance, although the National Aeronautics and Space Administration (NASA) and the Department of Defense (DoD) both fall under the category of *government*, their motivations for supporting research in quantum technology differ. Nevertheless, we broadly be classify an organization into one or more of these three categories.

2.2.1 Government and the public

The relationship between the public and the government is defined by an exchange of individual liberties for services and security [Loc90]. Introducing a new technology into this

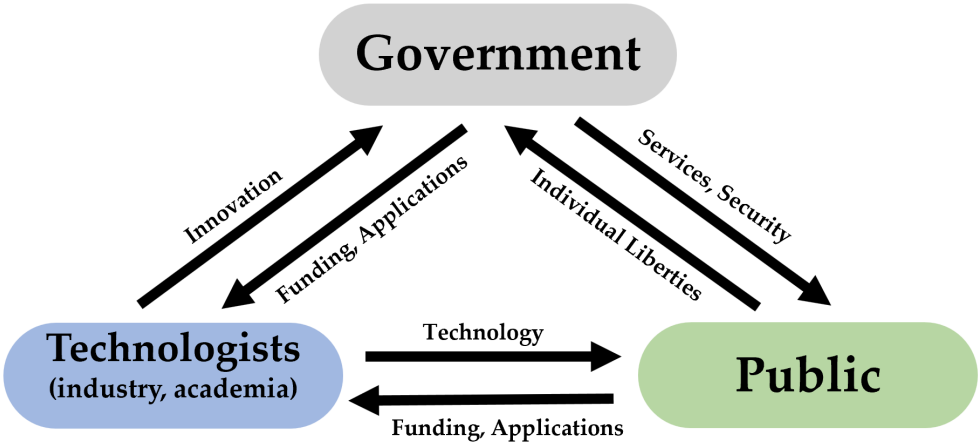

Figure 2-1: We create a stakeholder triangle for assessing the development of a technology and its impact on society. Each arrow points in the direction of what one stakeholder receives from another.

relationship may either strengthen or weaken the negotiating power of either stakeholder. For example, suppose that the National Security Agency (NSA) possessed a quantum computer large enough to break 1024-bit RSA encryption within seconds. If all messaging services used this encryption standard for their key exchange, then the government would be able to intercept every single end-to-end encrypted message and learn its content. In this scenario, the NSA's ability to effectively fight terrorism and provide security to its citizens greatly increased, but it also means that citizens would sacrifice some privacy in their digital lives.[2]

Occasionally the government and public will share the same interests, but not always. In determining stakeholder relationships, we see that a technology's ability to shift the balance of power does not bring about conflict *until* stakeholder interests become misaligned. If the government and public disagree on how society should be governed, then tensions will flare; if they do agree, then there is no need for instigating a conflict about which party possesses too much power. An example of where this tension flares is in the use of machine learning for predictive policing [Ame+16]. The public criticizes such algorithmic decision-making for reinforcing the biases of society, whereas the police argue that the technology is keeping crime-rates low because it is an effective tool for predicting recidivism rates.

[2]Note that this imbalance does not always shift in favor of the government. If we were to instead introduce an eavesdrop-free quantum network for consumers, then the power balance could shift in favor of the public.

The government-public relationship can be characterized by answering the following questions: how much trust does the public have in the government to act effectively and in their best interest? What liberties are they willing to exchange for government services? Finding the equilibrium point in this power dynamic will depend heavily on a country's model of governance.

2.2.2 Technologists and the public

We now transition to the monetary relationship that the public has with technologists, both in academia and industry. The public funds projects with an application in mind and technologists are expected to output something in return that improves everyday life. For example, JP Morgan Chase (the public in this scenario) recently partnered with Honeywell (the technologist) to fund the development of their new quantum computer [Pin+20]. In exchange, JP Morgan Chase gets access to a quantum computer that may improve the firm's computational power and garners public favor by investing in the technology's development.

Again, we see that conflicts due to imbalances in power arise when stakeholder interests are not aligned. For example, Facebook and the public are in nearly constant disagreement regarding how the platform monetizes user data. The social media company is frequently the subject of criticism for not respecting the privacy of its users, who feel they have little to no control over how their data is handled [Rai18], which has subsequently spurred several attempts by Congress to correct this imbalance by passing a privacy omnibus.[3] In this case, the technologist can be seen as not acting in the best interest of the public because they have a monetary incentive not to do so.

The challenge here is determining why technologists innovate. When public and government interests in developing a particular technology conflict, how do technologists reconcile this difference and how is their decision dependent on the relationship that a government has with its people?

[3]See: S.2968 - Consumer Online Privacy Rights Act introduced by Senator Maria Cantwell [D-WA] in 2019; S.3456 - Consumer Data Privacy and Security Act of 2020 introduced by Senator Jerry Moran [R-KS].

2.2.3 Government and technologists

Perhaps the most important relationship in our analysis is the relationship that the government has with its technologists. This exchange is similar to the public-technologist exchange, but with less of a consumer focus. One such example is the DoD's partnership with Army Research Laboratory (ARL) to develop a quantum clock network in the Washington, D.C. area [Com19]. The government is granting a large contract to ARL in the hopes that their progress in building a quantum clock network will help answer questions about scaling a quantum network. Eventually such a network could be used to connect quantum sensors around the world and improve domain awareness for the military. It is noted that ARL is officially a government organization. However, since they play a technical role in pushing the boundaries of QIS research, they are labeled as a technologist under this framework.

The tension here is a disagreement between technologists and the government over how their technology is used. A recent example of this is the petition that over 3000 Google employees signed in opposition to Project Maven, a DoD-funded project to improve image recognition software [Dea19]. A subset of technologists at Google did not approve of how the government could take their innovation in artificial intelligence and use it to improve drone-striking capabilities.

This relationship can be characterized by answering the following questions: does the government view technology primarily as a tool for effective governance or as a threat, or is the answer somewhere in between? How much trust do technologists place in the government to use a technology for the purpose they desire?

2.3 The U.S. quantum technology research landscape

In this section, our goal is to draw possible boundaries of collaboration with China by looking at how the U.S. approaches innovation in quantum technology. In order to understand quantum technology development through a political lens, we have constructed a view of the quantum technology stakeholder landscape, shown in Figure 2-2.

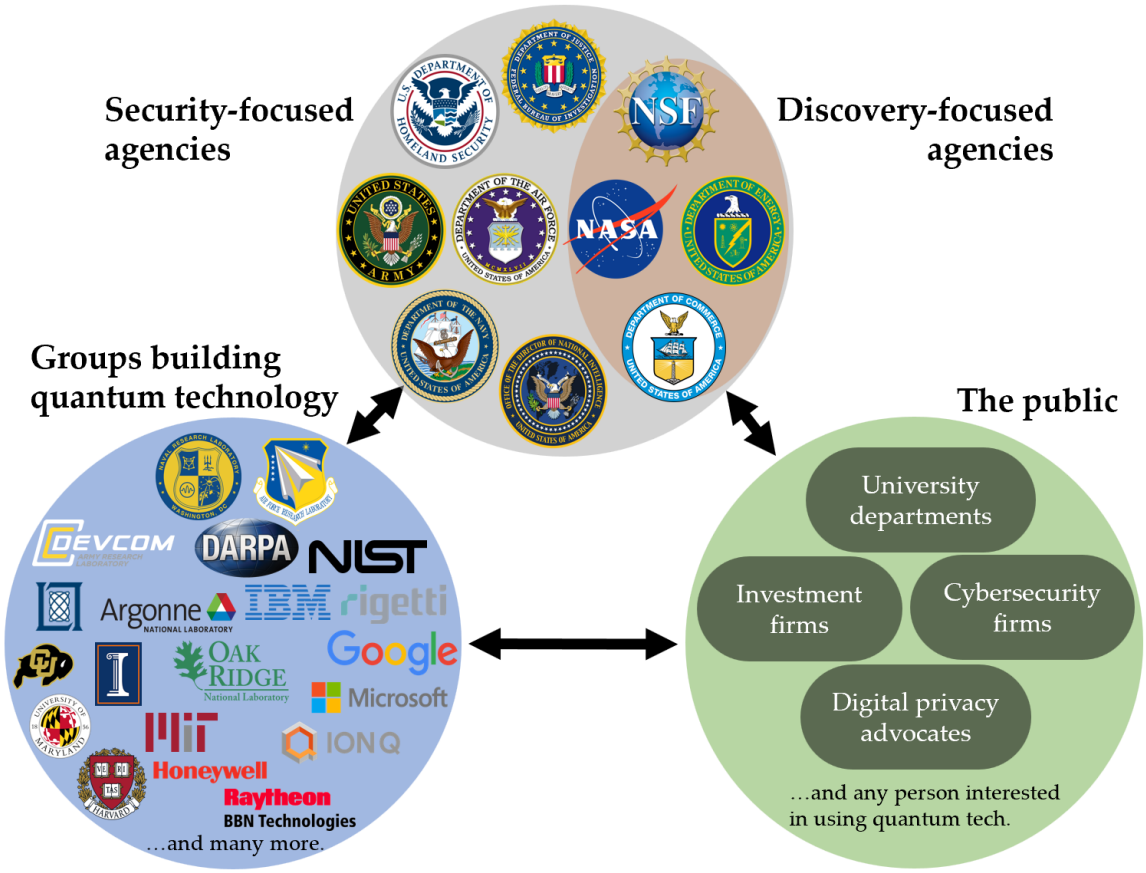

Figure 2-2: The U.S. stakeholder landscape for developing quantum technology. The groups in this diagram represent some of the major quantum technology stakeholders in the United States. Although each group within a particular category share similar desires, their motivations are not identical.

2.3.1 Government

It is estimated that the U.S. government spent $200-250M in 2019 on unclassified quantum information science (QIS) research [Fig18]. The federal agencies currently sponsoring QIS research include: the DoD, the Department of Energy (DOE), NASA, the National Science Foundation (NSF), and the Office of the Director of National Intelligence (ODNI), which includes the NSA. Other stakeholders that have a security interest in quantum technology include the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS). Finally, the Department of Commerce has expressed interest in QIS through the work being done by the National Institute for Standards and Technology (NIST) [KMW02], in addition to holding a 2018 Digital Commerce subcommittee hearing on its potential economic impact [WP18].

The government stakeholder is partitioned into two groups: federal agencies interested in quantum technology for security purposes and agencies who are interested for discovery and education purposes. The former group seeks to innovate and regulate quantum technology with the goal of improving the U.S. security posture, both domestically and abroad. Any desires to restrict public access to quantum technology or international collaboration will likely come from this group. Based on national strategy documents [Whi18; KG20] and the types of quantum research projects being funded [Off20a; Ric14; Com19], we can reasonably conclude that improving the ability to collect information and control it in a given domain — be it cyber, space, air, land, and sea — is of paramount importance to security-focused agencies.

Other agencies can also be subject to international collaboration restrictions by the federal government if their mission is deemed important to national security. Since 2011, the U.S. has banned NASA from hosting or collaborating with scientists affiliated with the Chinese government (Pub. L. 112–81), though an exception was made for China's Chang'e 4 mission because it was decided that the exchange of knowledge did not have any security implications [Dav19]. Given that advancements in quantum information science has the potential to affect either country's security posture, it is unlikely that Congress would make a similar exception for a joint quantum network project without a pressing need to do so. In Chapter 3, we will establish this exigency by analyzing the tenuous relationship between the U.S. and China.

2.3.2 Technologists

The federal laboratories that are, in some capacity, conducting research in quantum networks include: the Defense Advanced Research Projects Agency (DARPA), NIST, ARL, Naval Research Laboratory (NRL), Air Force Research Laboratory (AFRL), Argonne National Laboratory (ANL), Oak Ridge National Laboratory (ORNL), MIT Lincoln Laboratory, NASA research facilities, Los Alamos National Laboratory (LANL), Sandia National Laboratory, and Lawrence Livermore National Laboratory. Figure 2-2 also includes a few universities that have notable research programs for quantum communications: MIT, the University of Maryland, CU Boulder, University of Illinois (UIUC), and Harvard; they are illustrative representatives of what is actually a much larger number of academic institutions doing research in QIS. Finally, large technology firms and defense contractors are primarily focused on building quantum computers, sensing devices, and algorithms. Notable players in this group include: IBM, Google, Microsoft, Honeywell, Raytheon, Lockheed Martin, Rigetti, and IonQ.[4]

It appears that members of the technologist stakeholder group do not have strong motivations about access to quantum technology that may end up conflicting with government agencies, though quantum information scientists have testified in front of Congress before about the need for international collaborations in QIS [SCW17]. The mission of a national laboratory is consistent with that of its government sponsor, so motivations for innovating will be aligned. What this means in practice is a federal agency's policy on cooperation with China will cascade down into the type of research partnerships that its sponsored labs can pursue. Technology firms have also been recently affected by government interests, as discussed further in Section 3.1.3. They have been urged recently by the State Department to exercise caution in partnering with Chinese companies, citing concerns of intellectual property theft and the creation of dual-use technologies that can benefit the Chinese military [Pom20b].

2.3.3 Public

There appear to be four main groups within the public, as depicted in Figure 2-2, that will be a major voice for how quantum technology is used domestically:

1. Researchers interested in using quantum technology for their work. This group is strongly motivated to uphold academic integrity and prevent the theft of intellectual

[4]This is not meant to be a comprehensive list.

property;

2. Investment firms and other businesses who want to use quantum computing to improve their day-to-day operations. They desire unfettered access to quantum computing resources for their work, so they will push back on regulation that would weaken their ability to do fulfill this desire;
3. Cybersecurity firms wanting to provide security assurances to their clients. Quantum technology poses major threats — as well as opportunities — that will affect this group's ability to successfully do their job. They will be vociferous about any regulation or lack thereof that would threaten their client's security posture; and
4. Digital privacy advocates fighting against violations of the U.S. Constitution and consumer privacy. This group will advocate on behalf of U.S. citizens for legislation that protects an individual or company from being the target of abuses in power. If quantum technology can be used to intrude on the privacy of an individual or company, then this group will lobby for usage restrictions.

These communities will have minimal influence — outside of assuming an advocacy role — in establishing international scientific cooperation because the strategic implications of such a project, as discussed in Section 3.3, will likely make the process a tightly-controlled government-technologist endeavor.

2.4 China's quantum technology research landscape

We apply the stakeholder triangle framework introduced in 2.2 to the quantum technology landscape in China, depicted in Figure 2-3.

2.4.1 Government

It is estimated that the Chinese government invested approximately $240M annually from 2016-2019 into QIS research [Fig19], with over half of that dedicated to quantum communications and sensing for military applications [Zha+19]. Quantum technology has been listed as a major component of the 2030 S&T Mega Project in the Thirteenth Five Year Plan (2016-2020) [KC18]. Among the ministries interested in developing quantum technology for defense are: the People's Liberation Army Strategic Support Force (PLASSF), the Ministry of Industry and Information Technology (MIIT), the Cyberspace Administration of China (CAC), and the

Ministry of State Security (MSS). The other ministries that have a hand in its development are the Ministry of Science and Technology (MoST) and the Ministry of Commerce (MOFCOM). Finally, the National Development and Reform Commission (NDRC), responsible for economic planning in mainland China, is coordinating with provincial governments to deploy a national-scale fiber network for quantum information transport [Zha+19].

Two ways to discern the motivations of the Chinese government are by looking at publicly announced government-technologist partnerships and by translating the science and technology road-maps published every few years. The Party appears interested in promoting *civil-military fusion* in QIS research, a policy intended to lower the barrier for cooperation between technologists and the military (as well as defense contractors) [Las18]. This suggests that China primarily innovates for the security benefits that quantum technology can offer, which would be consistent with a 2018 report stating that China's decision to establish a national-scale quantum network — initiated in 2017 with the deployment of fiber between Beijing and Shanghai — came after initial documents leaked by Edward Snowden alleged that the U.S. was eavesdropping on communications within the country [KC18].

The Party's push for civil-military fusion in QIS should not be interpreted as an indication that China would oppose all scientific collaboration. Jianwei Pan, often referred to as the "Father of Quantum" in China [Led+17], treats quantum networking as a multilateral issue. In a 2018 interview with the *National Science Review*, Pan remarked, "We need quantum channels that are widely distributed and easy to use, including both fibre and satellite links. I can't imagine that any country can meet these challenges alone, without international cooperation." [Bal18] As discussed in Section 1.2, there are many non-military applications of a quantum network where international cooperation is mutually beneficial if not outright necessary, which China's quantum research leadership has acknowledged by *prima facie* expressing a willingness to cooperate with other countries.

2.4.2 Technologists

The technologists in China may be segmented into two categories. The first category is comprised of academics and defense contractors who innovate primarily for security applications [KC18]. Some of these organizations include: University of Science and Technology of China (USTC) at Hefei National Laboratory, the Chinese Academy of Sciences (CAS), the China Electronics Technology Group Corporation (CETC), the China State Shipbuilding Corporation

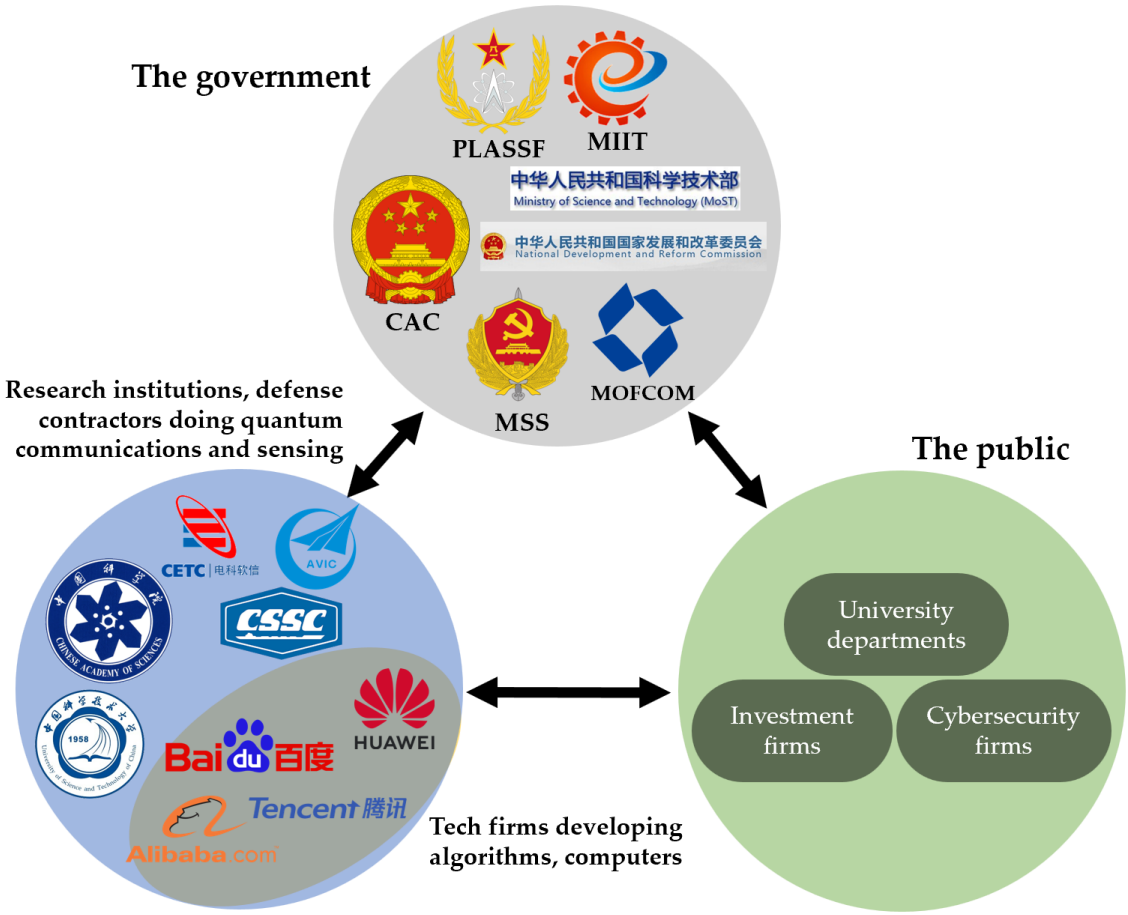

Figure 2-3: The stakeholder landscape for QIS research in China. Unlike the U.S., it seems that China concentrates its quantum research to within a few universities and large technology firms, who work closely the Party to create a road map for innovation. Gauging public sentiment towards research in quantum is also challenging because of well-documented issues with State censorship. [Bri10]

(CSSC), and the Aviation Industry Corporation of China (AVIC). The second group consists of companies focusing primarily on quantum computing and algorithms: Baidu [Whe20], Huawei [Yun18], Tencent [Li20], and Alibaba [Sun18].

The relationship between technologists in China and the Party is more intimate than that of the United States. The reason here is three-fold. First, as mentioned before, the Party is placing a greater focus on civil-military fusion in research, thus strengthening the bond between military, academia, and industry. Second, the educational mission of Chinese universities have become increasingly entwined with Party goals. Since President Xi came to power in 2013, over 100 universities unveiled a charter affirming their support of Party leadership for the first time ever [FC20]. Finally, the Chinese government is more open to financially supporting large-scale projects proposed by technology firms — such as the bicycle-sharing program [Gui14] — if they have the potential to improve the country's infrastructure and they do not interfere with the Party's ability to govern. Because the Party has forged a relationship with industry in this way, technologists and government in China present a unified front regarding how quantum technology in the country should be developed and deployed.

2.4.3 Public

We suspect that the public stakeholder groups for quantum technology will be the same in China as they are in the U.S., with the exception of digital privacy advocates. The Party has apparently not initiated any program for building a quantum-smart workforce beyond what was already being achieved through the Thousand Talents Program [Wan10]. Anecdotally, numerous discussions with colleagues who have ties to China have led us to suspect that information about quantum technology is not as widespread in the country as it is in the U.S., though supporting this claim would require a comprehensive cross-comparison between American and Chinese news outlets. Similar to the American public, we can conclude with some confidence that Chinese citizens would not push back against or advocate strongly for international cooperation, especially considering there are other more pressing issues, such as state censorship [Lor13] and tracking [MD18], that require attention.

2.5 Conclusion: defense-driven innovation

Military force modernization plays a major role for both the U.S. and China in choosing to invest in quantum information science, so an exchange of information will be scrutinized as a possible threat to national security. And since government-funded projects dominate the quantum technology landscape, technologist are not likely to pursue international collaboration without the approval of the government. Despite security concerns, a top QIS scientist in China has expressed an interest in collaborating with other countries [Bal18]; we might surmise that this view represents that of the Party given the close ties between academia and government in the country. Nevertheless, the Party may be apprehensive to a knowledge exchange with the U.S. for competitive reasons. The U.S., meanwhile, started closing off many opportunities for technology exchange with China in 2020, as we discuss in Section 3.1.3. Any laboratory funded by the DoD, DoE, or NASA is unlikely to receive approval to conduct a joint experiment with a Chinese researcher group without a major shift in the security policy as of 2020.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 3

Re-Imagining U.S. Tech Security Policy

In Chapter 1, we explored how a global quantum network would be useful for more than just defense purposes. However, Chapter 2 illustrated how the direction of QIS is still driven largely by the promise of improving a country's security posture, which holds true for both the U.S. and China even though their approaches to technological innovation differ. Any form of QIS collaboration — including those with zero ties to defense — will likely be heavily scrutinized by each country for the potential of divulging sensitive information. An agreement can likely only be reached if the U.S. and China are both confident that the benefits they receive outweigh the risks.

For the rest of this thesis, we are going to focus specifically on QIS cooperation from the U.S. perspective. In Section 3.1, we discuss how any potential for collaboration is further diminished by the fact that in 2020 U.S.-China relations have sunk to their lowest point in history. In Section 3.1.3, we explore how the tech sector has become a new arm in 2019 and 2020 for exercising foreign policy, thus adding an extra layer of controversy to collaborating in quantum technology.

If the government decides that quantum network collaboration is too risky, it assumes that their current approach to security policy is correct. In Section 3.2, we challenge this assumption by illustrating some flaws with the U.S. security posture. We assert that the U.S.'s

current diplomatic trajectory is guiding the country toward a future that will leave it in a vulnerable position. Finally, we propose an alternative approach to diplomacy in Section 3.3 built upon the foundations of U.S.-U.S.S.R. Cold War crisis avoidance and cooperation in space exploration.

3.1 Current U.S.-China relations are at a turning point

Strategic and economic dialogue between the U.S. and China is at a standstill. In 2006, the Bush administration chartered a framework for discussing economic issues with China semi-annually, called the Strategic Economic Dialogue [Dep08]. In 2009, the Obama administration renamed this to the Strategic and Economic Dialogue (S&ED) and expanded the role of the State Department in those conversations [Cli09]. This initiative was again renamed to the Comprehensive Economic Dialogue (CED) under the Trump administration in 2017, with the promise that similar meetings would be taking place at the same frequency as they did during the S&ED [Dep20d]. The last published CED meeting took place over two years ago, shortly after its establishment by Presidents Trump and Xi [Dep17a]. In January 2020, talks were reported to resume on a semi-annual basis as part of phase one in the new U.S.-China trade deal [Hol20]. However, July 2020 reports indicate that the administration is not considering phase two of the trade deal given that relations have worsened dramatically [ZL20].

The collapse of these dialogues comes as U.S.-China relations are at their lowest point in history in 2020 [Swa19; Sti19], sinking lower every day as tensions flair amidst the COVID-19 pandemic [MGB20; Off20b]. Ill-will had already built up on both sides well before the outbreak of COVID-19, but it has escalated to new levels in recent months. In June 2020 alone, Secretary of State Mike Pompeo made 12 press statements and gave 3 speeches (unrelated to the pandemic) denouncing the actions of the Chinese government, labeling the Party as an "authoritarian regime" [Dep20c]. The State Department has adopted a hawkish stance toward negotiations with China, proclaiming that "there is no compromise between freedom and authoritarianism" [Pom20a]. That is not to say the U.S. should refrain from criticizing the Party for their aggression in Hong Kong [BB20], Xinjiang [Mai20], and Ladakh [Get20], but the recent uptick in public denouncements from Secretary Pompeo himself illuminates a rise in the aggression of U.S. diplomatic tactics.

China seems to be equally discontent with the actions and statements of the U.S. government,

but it appears at first glance as though they are willing to return to the negotiating table. Fu Ying, former Vice Chair of Foreign Affairs and chairperson of the National People's Congress Foreign Affairs Committee, believes that the "China-U.S. relationship is at a turning point. Will it drift into a 'cold war' and the two countries become enemies to each other? Or will they establish a new-type of relationship via effective communications?" [Yin19] Especially during watershed moments like the aftermath of a global pandemic, the next steps taken by either country are pivotal to future geopolitical stability and will probably have decades-long consequences.

3.1.1 Minimal shared language for conflict resolution

The real danger of ending a decade-long dialogue with China is that, in the event of conflict, there are no established protocols for preventing further escalation. A standstill produces heightened tensions, which becomes an urgent issue when neither country has developed contingency plans for conflict resolution in the event that tensions flare. In contrast, the U.S. and Russia have established a number of direct communication lines, including the Washington-Moscow hotline used by President Obama to warn President Putin about meddling in the 2016 U.S. election [ADM16] and a 24/7 Nuclear Risk Reduction Center in each country — whose role been expanded to include notification about cybersecurity incidents as well [Off13]. Additionally, the U.S. and Russia continue to pursue joint space exploration projects, which has been an ongoing effort since 1962 [SE08].

The issue is that the U.S. and China do not have an array of long-standing protocols for conflict resolution and attempts thus far to establish them have been fruitless [Sti19]. A Washington-Beijing hotline was established in 2007, but its use has been mostly limited to space, air-to-air, and military encounters in the Asia-Pacific [Ste15]. The China Daily, a state-run media outlet, has advocated for expanding this hotline to include issues in cyberspace, but nothing has been done so far [Chi11]. The process of building bilateral vocabulary for crisis avoidance advances every time a new channel for dialogue is opened. And as we will discuss in Section 3.3, the example set by scientific collaboration between the U.S. and U.S.S.R. during the Cold War — while not quite a perfect analogy for the U.S.-China relationship — will provide valuable insight in understanding how a joint U.S.-China research project would impact the ability to resolve future conflicts.

3.1.2 The cyberspace geopolitical landscape

Further exacerbating mutual trust, the U.S. and China claim to have been repeatedly antagonized by the other in cyberspace. Probing an adversary's networks for opportunities to conduct espionage can stagnate progress made through official channels. The integrity of a deal comes into question when the actions of a state are inconsistent with the promises they make. Table 3.1 lists U.S. Department of Justice indictments made from 2014 to 2020 regarding Chinese cyber espionage. The Party has been less vocal about publicly calling out U.S. government-affiliated network intrusions, but the official Computer Emergency Response Team of the Chinese government (CNCERT) did publish a report last year claiming that the U.S. posed the biggest threat to Chinese network security, accounting for 53.5% of all intrusions in 2019 [CNC19]. In the same report they claim that 27.8% of network intrusions against China were motivated by espionage or sabotage. Given that the Chinese government likely reviews every piece of information published by a government organization, CNCERT's claim can be interpreted as the official stance of the Party regarding U.S. behavior in cyberspace.

The U.S.'s indictments and CNCERT's statistics are strategically very important, even if their veracity came into question. Both parties publicly claim to be the victims of incessant cyber attacks by the other. Public accusations and indictments are another instrument of power in a country's diplomatic toolbox [Sco18], acting as both a deterrent to future network intrusions and as a bargaining chip for garnering support from other countries [Tea19]. However, public accusations may also widen the already-growing diplomatic divide because such statements are adversarial in nature [GW18]. They may also be used as justification for adopting a more aggressive posture in cyberspace, causing further escalation.

U.S. offensive cyber capabilities

The U.S. and China have demonstrated that they are technically sophisticated enough to launch attacks with the ability to inflict significant damage a country's critical infrastructure. Experts and media reports have compellingly asserted that the U.S. was responsible for the 2010 Stuxnet attack, a sophisticated piece of malware that utilized four previously undiscovered ("zero day") exploits of vulnerabilities in the Windows operating system, in order to destroy nearly a thousand centrifuges being used to enrich uranium for Iran's nuclear weapons program [NW12].

Date		Unit/Individuals	Description	Source
2014	May	PLA Unit 61398 (APT 1)	Economic espionage	[Dep14]
2016	Mar	Su Bin	C-17 IP theft	[Dep16]
2017	Nov	Boyusec (APT 3)	Siemens, Trimble IP theft	[Dep17b]
2018	Sep	Yanjun Xu	MSS-linked theft of aerospace IP	[Dep18a]
	Dec	Zhu Hua, Zhang Shilong	MSS-linked 12-year long IP theft	[Dep18b]
2019	May	Fujie Wang et al.	2015 Anthem Inc. data breach	[Dep19]
2020	Feb	PLA 54th Research Institute	2017 Equifax data breach	[Dep20a]
	Jul	Li Xiaoyu, Dong Jiazhi	COVID-19 research IP theft	[Dep20b]

Table 3.1: List of U.S. Department of Justice indictments of Chinese cyber espionage from 2014 to 2020.

Per media reports, U.S. efforts to exploit vulnerabilities in critical infrastructure continue to this day. For example, a June 2019 article in the *New York Times* alleged that United States Cyber Command (CYBERCOM) emplaced malware in the control systems of the Russian electric grid, as part of a broader campaign to deter Russian interference in the 2018 U.S. midterm election [SP19]. Furthermore, General Paul Nakasone, Commander of CYBERCOM, posits that the U.S. can "achieve success [in cyberspace] by seizing the initiative, retaining momentum, and disrupting our adversaries' freedom of action." [Nak18] The word "disruption" is important here because it indicates an offensive posture, underpinned by engaging in sabotage of adversary systems.

China's offensive cyber capabilities

China's cyber capabilities are split across a number of entities, including the PLA and MSS, as well as scattered, decentralized "cyber militias," which conduct everything from propaganda to penetration of foreign networks on orders from the central government [Gre16]. While no Chinese attacks are believed to have caused physical damage to critical infrastructure, China's interest in sabotage remains clear: in August 2019, the cybersecurity firm Proofpoint reported that attackers believed to be associated with the MSS attempted to penetrate the networks of three U.S. utilities via a targeted phishing attempt [RS19].

Chinese-labeled cyber attacks have focused mainly on espionage. In 2013, Mandiant released a report on PLA Unit 61398 (labeled "APT1"), outlining their involvement in the theft of intellectual property (IP) through espionage, which was later confirmed by U.S. officials [Man13]. As a result, Presidents Obama and Xi came to an agreement in 2015 that "neither country's

government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information" [Off15]. A year later, FireEye published a report reviewing the activities of 72 cyber groups suspected of operating within China since the 2015 agreement. Their analysis showed that, although instances of network intrusion decreased in 2016, China was already making an effort to reduce the number of small hacks and consolidate their cyber talent as part of a larger military reform. From the report, "we see a threat that is less voluminous but more focused, calculated, and still successful in compromising corporate networks" [Int16]. And in March 2020, FireEye reported widespread attacks by a Chinese hacker group (labeled "APT41") across 20 different countries, noting it was "one of the most widespread campaigns [they had] seen from China-nexus espionage actors" [BS20]. Based on the FireEye's findings, it is prudent from a security standpoint for the U.S. to assume that there are organizations within China, such as the PLA Unit 61398 or APT41, that possess the ability to sabotage U.S. infrastructure even if they have not demonstrated such a capability thus far.

3.1.3 Information dominance and innovation isolationism

Information plays a significant role in contemporary geopolitics. It has become a tool for exercising soft power [Nye08] because it improves a country's ability to: influence other actors, make strategic decisions, create economic prosperity, and communicate effectively [RM19]. It is in a state's best interest to control and process the flow of as much information as possible by adopting a policy of *information dominance*, defined here as the ability to collect and handle any information that affects national security, while inhibiting an adversary's ability to do the same. Achieving *digital* information dominance in particular has become top priority because success in cyberspace is deeply intertwined with success in all other domains of warfare. The U.S. and China have both publicly claimed that information dominance in cyberspace is a strategic priority [Whi18; Cyb16; CR13], which their actions have supported.

But the policy of information dominance has manifested as more than just the ability to launch and prevent network intrusions; it has permeated into all innovation in the tech sector. The U.S. government has begun taking actions underpinned by a philosophy that can effectively be described as *innovation isolationism*: the U.S. government wants American innovation to stay domestic and Chinese innovation to stay out. Domestically, the U.S. government has begun heavily scrutinizing Silicon Valley for their role in developing technologies that affect national

security. In January 2020, Secretary Pompeo met with leaders of Silicon Valley, encouraging them to re-evaluate their business ties with the Chinese government and reminding them that export control restrictions will be placed on any U.S. technology that "goes into the CCP's nationwide surveillance machine," such as facial recognition software [Pom20b]. The Department of Commerce is also considering adopting a rule allowing them to block the sale of any U.S. technology tied to a "foreign adversary" [MS20]. Critics argue that such a policy would stifle innovation in the country and lead to a trend in start-ups relocating abroad, which in turn would decrease national security since many modern military technologies draw inspiration from commercial products.

In this framework for diplomacy, Chinese researchers and technology pose a greater risk than they do a reward. Internationally, the U.S. has also begun blocking many technologies and scientific endeavors coming from China that have Party ties, citing intelligence concerns. In the world of social media, the U.S. government has banned the use of TikTok, owned by Chinese firm ByteDance, on government cell phones [Hod19] and forced the sale of Grindr, a dating app recently acquired by a Chinese firm [San20]. Regarding critical infrastructure, the government has banned Huawei 5G towers [Kea20] and all Chinese electric grid equipment in the U.S. [Whi20]. In academia, the U.S. government is set to cancel the visas of all Chinese graduate students in the U.S. with ties to the PLA [WB20].

3.2 The current security framework has glaring vulnerabilities

Some of the actions taken by the U.S. government have been supported by rigorous threat analysis, but caution should be exercised when adopting a blanket ban on Chinese R&D — especially since the decision appears to be conflated with issues in U.S.-China trade policy — because it may lead to unnecessary escalation. As evidenced by the U.S.'s relationship with the U.S.S.R. during the Cold War, the U.S. can cooperate in good faith on certain issues — space exploration, for example — while uncooperative on others. However, any chance to have a say in China's decision-making process may be lost if they are cut out of the U.S. ecosystem entirely.

Underpinning the current technology isolationist policy is a belief that the U.S. can innovate out of any problem that may arise, without the help of China. For example, the U.S. may believe it can operate the country's infrastructure without Chinese technology and maintain

the status as the global leader in research without Chinese scientists. Should U.S.-China policy continue down this path, these statements may turn out to be true. However, as outlined this section, we claim that that the U.S. will not be able to solve all of the country's security problems without a stable relationship with China.

U.S. relations with China have never been worse than they are in 2020, as discussed in Section 3.1. A hard-line approach to diplomacy can act as a deterrence, but it can also put the country at an even higher risk than before. We claim that 2020 is not the year to begin creating an innovation divide between the U.S. and China. We challenge the notion that the U.S. can solve all their security issues without building bilateral stability with China. We support this by highlighting three security problems the U.S. is dealing with right now — each different in scope — that all point to cooperation as the solution.

3.2.1 State threat: how suspicion festers in cyberspace

The risk presented by adopting an aggressive posture toward China is that it may increase the probability that a tactical decision made under imperfect information will further escalate the situation. This can lead to disastrous consequences, including the potential for loss of life. Difficulty in determining when exactly an adversary is preparing to launch an attack is not a new problem brought on by the creation of the Internet, but it is one that is exacerbated in cyberspace. Ben Buchanan outlines in his book, *The Cybersecurity Dilemma*, several factors that contribute to the propagation of distrust between states in cyberspace [Buc17]. Because it is so hard to detect every foreign intrusion on a network, Buchanan argues that states will conduct their own offensive operations in order to collect intelligence on both adversaries and allies alike. But this problem is compounded by two factors: 1) most of the work in launching an attack happens during the network intrusion phase and 2) it is difficult to tell the difference between a defensively and offensively motivated network intrusion. A defensive-minded state must operate under the assumption that an intruder is preparing to launch an attack, but if they miscalculate the intentions of the intruder then they can become the instigators of conflict.

Mutual concern is also amplified by a basic network security principle: assume an intruder is already present in the system. As Buchanan notes, it takes significantly longer to access a network without authorization than it does to deploy an exploit and oftentimes an intrusion can serve as a landing point for future operations. If both countries are operating from the

assumption that the other has already prepared the environment, then they must conclude that the other can initiate an attack at a moment's notice. Moreover, even if a country is able to instantaneously determine that an intrusion was defensive-minded, they may still be inclined to retaliate because such an intrusion could be used a beachhead for future attacks and the defender cannot discern the true intentions of the hacker.

This mounting suspicion can be mitigated by developing some level of predictability in the actions that a state takes in cyberspace, effectively creating a set of confidence-building measures (CBMs) for cyberspace. CBMs were first developed during the Cold War when the U.S. and Russia were faced with the existential threat of nuclear warfare due to miscalculation. A CBM can be anything that signals to an adversary that a state is acting in a predictable way, such as the Washington-Moscow hotline or the publishing of troop movements and exercises. Regardless of the form that it takes, CBMs can work properly when there is bilateral stability and open channels of communication, which the U.S.'s current security posture towards China does not promote.

3.2.2 Non-state threat: destabilizing forces in cyberspace

Bilateral stability is also important in areas where there is concern about the threat posed by non-state actors. Buchanan's formulation of the cybersecurity dilemma largely ignores the destabilizing forces of non-state actors, which are more prevalent in cyberspace than in other geopolitical domains. Off-the-shelf tools for penetration testing — such as those native to the Kali Linux distribution [Kal19] — are widely available to the public and any individual who wishes to clandestinely develop an exploit can do so with relative ease. This is in contrast to the highly regulated process of traditional arms control, in which weapons development and compliance are heavily monitored [BL18]. Also present is the constant challenge of determining attribution in cyberspace, which some experts argue is brought on by the fundamental architecture of the Internet [RB14].

Regardless of whether or not attribution is more challenging in cyberspace than other domains, the mere existence of problems in attribution complicate any interstate signaling in the event of escalation between the U.S. and China. Fear and suspicion between two states in cyberspace are thus compounded by the destabilizing presence of non-state actors. Because signaling and arms control are more challenging in cyberspace, we argue that states should work in elucidating their intentions so as to avoid retaliation prompted by a strategic miscalculation.

Doing so could also facilitate their ability to properly address non-state threats in a timely manner. The destabilizing presence of non-state actors only increases the urgency with which the U.S. and China should seek improved diplomatic relations.

3.2.3 Global threat: the advent of multilateral security challenges

We assert that bilateral scientific collaboration is pivotal to improving the U.S. security posture because it can facilitate progress towards addressing several important global security issues. STEM research continues to become more cooperative around the world, especially in the fields of astronomy and physics. According to *Nature*, the average number of authors listed on an academic paper jumped from 10 in 2014 to 37 in 2015-16 for the physical sciences [Mal18]. That number continues to rise every year because of advances in networked science and data availability. Although the innovation isolationist behavior displayed by both countries recently may indicate otherwise, the U.S. and China have recognized this trend in the past and the importance of cooperation in space, each independently partnering with the European Space Agency (ESA) in recent years [Eur16; Eur19]. Past sentiment gives us a reason to believe that the two countries still share a common interest in working together to solve the global issues of today.

Innovation plays a large part in the ability to mitigate today's global security challenges which no country can unilaterally solve. For example, climate change can be slowed through global deployment of clean energy and carbon capture techniques. Expanding multilateral channels of information sharing for biomedical research could quicken the pace at which vaccines are developed in the event of a global pandemic. Coordinating efforts between NASA, ESA, CNSA, and other space agencies can improve the collective ability to remove space debris from low Earth orbit (LEO). Information sharing between Computer Emergency Response Teams in different countries could strengthen a government's ability to prevent and recover from cybersecurity attacks from non-state actors. Cooperation in technology development is one brick on the road to a more secure future.

3.3 U.S. security policy re-imagined through the lens of quantum networking

Let us consider an alternative security framework, underpinned by science diplomacy, where the U.S. and China come together to collaborate on global technology challenges and slowly build up needed bilateral stability. Science diplomacy should not be treated as a panacea for U.S.-China relations, as regular interactions between low-level members of each country cannot fully replace the strategic and economic dialogues between top-level officials. Here, scientific cooperation is being promoting as one of many ways that the two countries can communicate with one another given that said dialogues are currently in limbo. The power in science diplomacy is the initial symbolism of partnership and the slow building of trust over time through shared accomplishments.

3.3.1 Why we might want to choose quantum networking

The creation of a functional quantum network does not solve an urgent security risk like the global challenges mentioned in Subsection 3.2.3. Perhaps collaboration in this field should be put aside until the U.S. and China can resolve more pressing issues. Our rebuttal to this critique is twofold. First, working on a joint quantum link can still beget positive security externalities by improving scientific collaboration between the two countries with the highest academic throughput in the world. Despite the reports from a 2019 *Nature Index* showing that the U.S. is China's top collaborative partner, it is unclear if the U.S. government currently has any official scientific partnership with China [Woo19]. Official cooperation needs to start somewhere and there is a lot that can be learned about the U.S.-China research dynamic through a joint quantum networking project. Additionally, we argue that a quantum networking project poses a relatively low risk of inflaming bilateral tensions compared to a joint research project addressing a global security challenge, whose progress would have a direct impact on the lives of individuals. If something goes wrong on during the development of a quantum network, there may be financial or IP implications, but lives are less likely to be directly at risk.

Second, a joint quantum network could be symbolically powerful. QIS has been touted as the marquee field of research that will usher in a new future, a claim supported by the applications discussed in Chapter 1. A quantum link could be a physical connection between the U.S. and China. Its establishment would represent a renouncement of the old framework in favor of a

new one built on mutual interest in solving global issues. Quantum information is currently treated with extreme caution. The U.S. has subjected its international distribution to export control review (15 C.F.R. § 730 et seq) because of its security properties. But if the U.S. were to share a quantum link with China, it could mean setting aside concerns over the security threat quantum information poses in an bilateral effort to focus on the innovation that it promises, which we believe could be incredibly symbolic.

3.3.2 Why we might not want to choose quantum networking

We anticipate that quantum technology will play a major role in how the U.S. military operates in the future, a claim suggested by the innovation landscape we outline in Chapter 2. A core principle of the U.S. government's Third Offset Strategy [Fio16] — which seeks to maintain a military advantage over potential adversaries while preserving peace — is to outmaneuver others through innovation. Quantum technology may become pivotal in the success of this strategy because, as discussed in Section 1.2, it can enable advancements in domain awareness that could give the U.S. an asymmetric military advantage over China. Collaborating with China on QIS research may reduce the U.S.'s ability to successfully carry out this strategy because it could level the quantum technology playing field through regular information exchanges. Therefore, a joint quantum project may weaken the U.S.'s ability to deter. Deciding whether to pursue a partnership specifically in quantum may ultimately become an exercise in striking the optimal balance between deterrence and bilateral stability.

In addition to the challenge of deterrence, the U.S. may express concern over how dangerous a joint quantum networking project could be from an intelligence standpoint. As raised in Section 3.1.3, information is power in geopolitics. To estimate the risk that the U.S. government assumes in a joint quantum partnership with China, we must look at the specific project being proposed and assess what information China could learn about the U.S.'s quantum capabilities that would in turn put the U.S. at a greater risk than before. This concern is addressed in Section 4.4.

3.3.3 Drawing from principles of U.S.-U.S.S.R. science diplomacy

After John Glenn became the first American to orbit the Earth in 1962, Presidents John F. Kennedy and Nikita Khrushchev opened discussions for cooperating in the development of weather satellite technology and early satellite communications [SE08]. The partnership

grew increasingly intimate over the following years, including the symbolic 1975 Apollo-Soyuz joint docking mission and subsequent handshake that marked the end of the space race. To this day, the U.S.-Russia scientific partnership has remained strong, as illustrated by NASA's requirement for American astronauts to learn Russian (and vice versa) so the countries can communicate with one another during multilateral missions to the ISS.

The early years of cooperation, however, were less fruitful than either side hoped due to organizational differences and a sense of distrust stemming from early Cold War relations, according to Russian cosmonaut Roald Sagdeev [SE08]. Even the Apollo-Soyuz Test Project 13 years after cooperation began was a tightly-controlled endeavor because the Russian organizations involved were kept as secret as possible. Despite these setbacks, the partnership was considered a success for promoting the stability of space and improving bilateral communications. U.S.-U.S.S.R. efforts to collaborate in space were built on the same principles that would underlie U.S.-China collaboration: the gradual building of trust between scientists in both communities, establishing trusted channels of communication, and signaling a desire for stability.

As for their lasting impact on future diplomacy, it should be noted that, even while U.S.-Russia relations were near their nadir in 2018, the heads of the Russian Main Intelligence Directorate (GRU), Foreign Intelligence Service (SVR), and Federal Security Service (FSB) travelled to Washington, D.C. to meet with the Director of the CIA on continuing bilateral cooperation on counter-terrorism efforts [WL18]. The fact that these two nations continued to work together towards a common goal while relations were distressed suggests that the early work put into improving bilateral communications during the Cold War — a core principle of science diplomacy — can work in practice. The hope is that QIS collaboration can induce similar positive externalities for future stability.

Of course, the analogy is not perfect. U.S.-U.S.S.R. collaboration on space exploration was motivated by the existential threat of nuclear warfare. The floor for instigating conflict is significantly higher in nuclear policy than it is in quantum policy because one intercontinental ballistic missile, which could be launched at any moment, could wreak havoc on the lives of millions. Its potential for destruction dwarfs that of any existing quantum or cyber weapon. Additionally, the introduction of anti-ballistic missile technology emboldened states to act aggressively because it presented the guise of invulnerability [Off19]. It is unlikely that a future quantum technology, including a computer large enough to crack RSA encryption,

will induce a similar brazen disregard for restraint in any domain of warfare. Nevertheless, Cold War crisis avoidance doctrine is a good starting point for understanding the security externalities that a U.S.-China quantum network collaboration might produce.

Building relations between scientists

Science diplomacy connects technical experts from both countries through a formalized exchange of information. As a result, Chinese quantum researchers will retain a positive impression of their American counterparts (and vice versa). The central adversary in a joint scientific project is nature, not fellow scientists. This artifact of person-to-person exchanges was a guiding principle of U.S.-U.S.S.R. diplomacy during the Cold War. Former U.S. Ambassador to the Soviet Union Jack Matlock argued that scientific exchanges between the U.S. and U.S.S.R. were the foundation for effective diplomacy because they also built lasting interpersonal connections that would influence future decision-making [Kra19]. Differences were set aside in pursuit of a common goal. Space exploration was deemed technically challenging enough that even tightly controlled collaboration was of scientific and diplomatic use to both countries. Along the same lines, the challenge of building a global-spanning quantum network can be mitigated through cooperation, which would lead to spillover effects in stability by improving relations between scientists.

Establishing trusted channels of information sharing

Positive relations between scientists could prove to be extremely valuable in the event that tensions flare by offering a trusted, regularized channel for information sharing and uncertainty clarification. Quantum researcher relations could be used as a bridge for de-escalation during moments of crisis related to the field. Additionally, in the event that dialogue through main diplomatic channels prove fruitless, the quantum information channel can be used to further progress negotiations through Track Two (or "back-channel") diplomacy. Such dialogues between Iran and the the U.S. were pivotal in establishing the Joint Comprehensive Plan of Action (JCPOA) for nuclear nonproliferation when heads of state could not rely solely on the trust of one another [SB15; Kem14]. It seemed senior officials in Iran did not trust technical proposals put forth by the U.S., but Iranian scientists did trust the work of their American counterparts, which allowed the negotiations to move forward.

Stability signaling to the rest of the world

Scientific collaboration also doubles as a form of geopolitical signaling. Bilateral cooperation communicates to the rest of the world that the U.S. and China are interested in promoting stability, especially considering how both countries treat QIS research as an opportunity for military force modernization. A joint project would have cascading effects on the actions taken by other countries that choose to cautiously escalate their security posture during times of uncertainty. In collaborating on space exploration, the U.S. and U.S.S.R. were signaling to other countries their interest in keeping space free from militarization, which helped lead to the signing of the Outer Space Treaty by 107 other countries [Off67]. The decision to formally collaborate underpinned security agreements during the Cold War that would go on to provide decades of geopolitical stability.

The role of the U.S. and China as leaders in quantum information science cannot be understated. As discussed in Subsection 3.3.1, a quantum collaboration is symbolically powerful. A U.S.-China project could signal a desire for stability in both space, through which quantum information will be transported, and cyberspace. It would illustrate a marked shift from the current self-reliant, hegemonic security strategy to a new willingness in forming bilateral partnership to solve today's global security issues.

3.4 Conclusion: bilateral stability is necessary to improving national security

The U.S. is at the most important juncture the country has ever faced regarding its relationship with China. Strategic relations have sunk to new lows in 2020 amidst the COVID-19 pandemic, new accusations of cyber espionage and IP theft, and ongoing trade disputes. The U.S. government has responded by adopting a series of escalatory policies for ridding the U.S. tech sector and academia entirely of Chinese innovation. The U.S.'s current policy trajectory indicates that the government firmly believes in their ability to improve national security without building a relationship with China.

In this chapter, we argued that this belief is inherently flawed by highlighting three instances in Section 3.2 where bilateral stability is pivotal to the U.S. security posture. First, we discussed how bilateral stability could facilitate the creation of confidence-building measures in

cyberspace for escalation prevention. Next, we analyzed how non-state actors are a destabilizing force that can hinder any state attempts at signaling intentions in cyberspace. Finally, we examined how solving future global security threats such as climate change and space debris may require bilateral scientific cooperation. We argued that a joint quantum networking project could a good starting point for rekindling relations because of its high diplomatic reward, but it may also threaten the U.S.'s ability to carry out the Third Offset Strategy [Fio16] given that quantum technology is likely to play a key role in military modernization.

Chapter 4

A Framework for U.S.-China Quantum Network Collaboration

In Chapter 3, we argued that the U.S. government's current isolationist approach to scientific innovation may not adapt well to an ever-evolving threat landscape that is both individual and global in scope. It could be in the U.S.'s interest to promote QIS cooperation with China because, in addition to accelerating scientific discovery, such a partnership could improve the country's security posture in the long run by re-establishing a bilateral link for conflict resolution that had previously been severed.

In this chapter, we propose a hypothetical framework for establishing scientific collaboration between the U.S. and China in building an international quantum network by discussing potential stakeholders (Section 4.1) and by identifying policy and technical outcomes for this collaboration (Section 4.2). The power of this research project is in the symbolism of distributing quantum information — whose security properties have made it a hotbed for discussion about export control regulations (15 C.F.R. § 730 et seq) — through outer space, whose perceived militarization has become a major point of tension in U.S.-China relations.

We also address some of the policy (Section 4.3) and intelligence (Section 4.4) challenges that may arise in this collaboration. Research laboratories learn a great deal about each other's technical capabilities in joint projects such as this one. However, not every piece of

information learned by their Chinese counterparts will pose an urgent security risk, similar to how joint space exploration missions with the U.S.S.R. did not significantly threaten the American nuclear posture in the Cold War [SE08]. We analyze what the U.S. and China could learn about the capabilities of one another in building a bilateral quantum link to show why the intelligence aspect may not be a cause for concern.

4.1 Potential stakeholders

One potential candidate for U.S. involvement in this cooperation is MIT Lincoln Laboratory (Lincoln), located in Lexington, Massachusetts. Throughout the lab are experts in optical satellite communications, entanglement distribution, ion trapping, and quantum sensing. The laboratory has also begun building up a quantum network between itself, MIT campus, and Harvard using a combination of quantum memories and photonic links [Gre+17; Zha+18]. It has strong ties to both universities and regularly conducts joint research [Lee+18; Bun+18].

The laboratory potentially best suited for international collaboration in China is Hefei National Laboratory for Physical Sciences (Hefei), in the Anhui province of China. Hefei has become the nexus for quantum information science research in China, with the best access to scientific talent and resources. It is also home to the research group of China's leading scientist in quantum communications research, Jianwei Pan, who has publicly expressed interest in collaborating with other countries [Bal18].

Both laboratories have strong links to military innovation. Lincoln is a DoD federally funded research and development center and Hefei National Laboratory is responsible for constructing one of the first metropolitan QKD networks in China [KC18]. One might criticize this as an immediate non-starter for any type of cooperation because both groups are linked too closely with national security interests, but this is one reason why these two labs could be strong candidates for a joint project. The diplomatic purpose of this collaboration would be for both countries to set aside some of the security risks associated with a scientific exchange in an effort to find common ground for future diplomacy. Establishing a partnership between two military-funded laboratories — instead of two research groups who do not have ties to the government — amplifies the stability signal of this collaboration.

As discussed in Section 1.4, a near term quantum link may "exist" through satellite relay,

so the government organizations potentially involved in this partnership include NASA and CNSA. A major roadblock worth mentioning is that a federal appropriations act passed in 2012 prohibited the use of any NASA funds for conducting a joint project with CNSA, which is a policy that remains in place today (Pub. L. 112–81). We recommend that this policy be revisited along with the ones adopted in 2019 promoting innovation isolationism, as discussed in Section 3.1.3. Finally, it is expected that the DoD could want to provide input into this partnership given that they are the primary funding source of Lincoln.

4.2 Goals for collaboration

Diplomatically, the goal of this framework could be to promote innovation and geopolitical stability through regular exchanges of knowledge that increase the scientific intimacy between QIS communities in both countries. Keeping each stakeholder's research goals in mind, we propose establishing a two-node link for sharing entanglement between the U.S. and China. It could enable many of the projects discussed in Chapter 1 and quantum link could also symbolize the forming a new connection between two countries that are willing to work together in addressing the challenges posed by emerging technologies. We anticipate that sharing entanglement between the U.S. and China would require relaying qubits through low Earth orbit. As we discuss in Section 1.4, quantum repeater technology is still in its infancy and it may never reach the point where it is robust enough to withstand the environmental fluctuations of the ocean floor. Because of the maturity of free-space optical links in near and low Earth orbit [Bor+09], it seems reasonable to assume that a near-term long-distance quantum network would also utilize free-space links.

Link stabilization may play a major part in the success of this project. A quantum channel is sensitive to phase, amplitude, and polarization noise. To overcome these challenges, researchers involved may have to learn a great deal about the best methods for stabilizing a quantum link. However, this is not an impossible task. Lincoln has demonstrated the ability to establish an optical communications link to as far as the moon through their Lunar Laser Communications Demonstration (LLCD) [Bor+09], while Hefei has experience directly transferring qubits over long distances through Micius, a satellite in their Quantum Experiments at Space Scale (QUESS) mission [Lia+17]. In Chapter 5, we discuss the fiber characterization work we have been doing at Lincoln which could help inform some of the challenges associated

with link stabilization.

4.3 Policy challenges

When it comes to a joint research project, we should keep in mind that it is not one lab versus another in a race to outpace the other in innovation; it is both labs versus nature. We do not have to look very far to find examples, such as the ISS and CERN, where this type of mentality during a joint project can pay off in a huge way. In this section, we discuss several policy challenges that may manifest in a scientific collaboration. The first is a misalignment in motivations, which results in a disagreement over the timeline or overall direction of a project. The second point of tension is one of resource control. Finally, we look at the relations of all stakeholders, both technical and non-technical, involved in the project.

4.3.1 Motivation misalignment

A stakeholder, as defined in Chapter 2, may not agree to put time and effort into a joint project unless they are certain they could either: 1) learn something new, 2) improve an existing method, 3) gain access to a useful resource, or 4) generate notoriety for their accomplishments. We anticipate that this criteria would need to be satisfied for a majority of stakeholders involved before any resources can be invested into the project. Responsibilities may need to be tentatively delineated up front to minimize miscommunication. This means that the amount and nature of work put into a joint project would need to be agreed upon by both parties. Lincoln and Hefei have their resources spread across a number of different projects. So, they cannot focus all of their time and effort into the collaboration. One potential way to ensure the project moves forward steadily could be by having one or more researchers from each lab dedicate most of their efforts on its accomplishment, assuming each lab has the time and resources available to do so.

4.3.2 Resource control

A quantum channel can be viewed as a common-pool resource [Ost15] because it could be used for multiple projects at any given moment following its establishment. So, the control of signal traffic may become an important topic in a joint quantum project. Resolving signal traffic issues in resource control is likely dependent on the channel being used to distributed

quantum information. For example, previous experiments over fiber have been conducted to better understand how a quantum signal is affected when multiplexed with a strong classical signal [Pet+09; Cha+09], but it is unclear if this same behavior arises in a free space channel. Some of these issues can be resolved technically, but it may also require strong coordination between both laboratories over what experiments should be prioritized. This could be a problem for any quantum network created, so it might prove useful to study this dynamic a joint U.S.-China quantum link. We anticipate that resource control is a topic that both laboratories may need to revisit intermittently so they are on the same page about what research projects the quantum link can be used for.

4.3.3 Stakeholder relations

The stakeholders affiliated with the research project — either directly or indirectly — must be willing to put their name on it. This may be an issue for a U.S.-China link given that politics are likely to play a major role in the decision to go through with a joint project. Any number of political events could affect the status of the project, such as a change in administration or the start of a new trade dispute. Overcoming the threat posed by worsening stakeholder relations starts with a commitment from every party involved that they will continue the project because they firmly believe in the benefits that it can bring regardless of how the U.S.-China strategic dialogue progresses. Over time, the U.S., China, Hefei, and Lincoln could all need a constant reminder (likely from the same one or more scientists spending most of their time and effort on the project) that the endeavour is still worth pursuing. As discussed in Section 3.3, the political will to continue this project may come from an appreciation of the bilateral stability built by regularized low-level dialogues between quantum information scientists in both countries.

4.4 Intelligence concerns

Information exchange is inevitable in a joint collaboration of this type, but it may not always be a security risk. To determine exactly what level of risk the U.S. assumes in this collaboration, we need to examine what Hefei learns about Lincoln. In working toward sharing entanglement, Hefei could learn, among other things:

- The distance and precision with which Lincoln can optically communicate via satellite

and the techniques associated with the process;

- The quality of laboratory equipment Lincoln possesses, such as lasers, detectors, and entanglement sources;
- The maturity of Lincoln's quantum repeater technology;
- The quantum protocols currently of interest to Lincoln;
- How Lincoln compensates for channel instability;
- Lincoln's problem-solving approach to building a quantum link and what they prioritize as important milestones; or
- The expertise of researchers at Lincoln.

Given that QKD has been dismissed as by prominent security agencies as a worthwhile investment [NCS20], it appears that the field of quantum communications is trending toward the promise of enabling advancements in metrology and domain awareness. One security risk this collaboration might pose to both countries, then, is that it could the other country's ability to connect quantum sensors into large scale arrays for military applications. This concern merits further investigation as sensor technology develops, but it may be too early to predict exactly how the methods learned during joint project will become the lynch pin for success in China's future pursuit of quantum sensing networks. Additionally, we should recall the diplomatic benefits of scientific collaboration outlined in Section 3.3. There is a great deal of interplay between improving relations and opening channels of information sharing. Improving strategic relations can lead to more channels for the flow of intelligence, but the same can also happen in reverse. This idea is the foundation for building some form of bilateral stability between the U.S. and China.

Exchanges in personnel and intellectual property have the potential to bring about further conflict. The U.S. government has expressed concern over the Party's strategy of recruiting top technical talent from around the world to conduct research in China, known as the Thousand Talents Program [Leo19]. Since Hefei could learn something about the expertise of Lincoln personnel, there may be a chance that the Party offers major incentives to select Lincoln researchers in exchange for relocation to China. Additionally, there may be intellectual property concerns associated with quantum network collaboration that need resolving. Disagreements in how each country treats IP has become a sticking point in the larger U.S.-China trade dispute initiated in 2018 [He19]. As illustrated by the DoJ indictments made since 2018 (Table 3.1), the U.S. government has adopted an aggressive posture towards IP theft from Chinese actors. De-

tails about publishing and patenting rights for technologies developed during a joint quantum project may need to be negotiated thoroughly in the early stages of the partnership.

4.5 Conclusion: a joint quantum project would be a trade off

The stakeholders involved in a joint quantum project could learn a great deal about how to transport quantum information, which may become valuable in quantum networking experiments done entirely domestically as well. For the U.S., the link stabilization methods developed during this project could become pivotal in eventually connecting the regional quantum networks being developed across the U.S., as described in the Department of Energy's "quantum internet" blueprint released in May 2020 [Kle+20]. The security trade off, however, is that the same may be true of China's ability to connect quantum devices. Ultimately, the decision to establish a research partnership depends on each country's willingness to set aside some of the intelligence concerns associated with a joint quantum project. We anticipate that, beyond intelligence concerns, the two countries are likely to encounter policy roadblocks along the way that slow the progress of a joint project. Nevertheless, as we discussed in Chapter 3, a joint quantum project has the potential to provide much needed stability to the current U.S.-China relationship and it could improve the U.S.'s ability to solve issues of national security.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 5

Case study on the MIT-Lincoln Quantum Link

Should the U.S. and China agree to a joint quantum project whose goal is the sharing of entanglement, it will likely become important that they understand the behavior of the quantum channel before engineering systems to achieve their goal. Qubits traveling over deployed fiber and free-space links may behave differently than they would in a laboratory environment. In this chapter, we describe work done with Group 67 at Lincoln in establishing a collaborative partnership between MIT campus and Lincoln, connected by a deployed 43 km fiber link. This work could help inform some of the technical challenges the U.S. may face under the framework for quantum collaboration we propose in Chapter 4. In Section 5.1, we discuss the 43 km deployed optical fiber link connecting Group 89 to Isaac Chuang's MIT Quanta Lab (Quanta) at the MIT Center for Ultracold Atoms (CUA). In Section 5.2, we present optical characterization of a 450 m segment of the installed optical fiber connecting laboratories in Group 67 and Group 89. And in Section 5.3, we describe future work that could be completed over the link.

5.1 A brief overview the MIT-Lincoln link

The MIT-Lincoln quantum test-bed is an optical fiber link that connects multiple sites, including Dirk Englund's Quantum Photonics Laboratory at the MIT CUA and Mikhail Lukin's Quantum Optics Laboratory at the Harvard CUA. For this case study, we focus solely on the portion of the link that travels through Group 67, Group 89, and Quanta.

Group 89 and Quanta work intimately with one another and specialize in building ion traps, while Group 67 focuses more on developing methods for optical communications, both classical and quantum. A partnership was formed between between Group 89/Quanta and Group 67 in 2016 because there was interest in exploring methods of quantum clock synchronization that could enable future quantum networking applications.

5.1.1 The Lincoln-MIT segment

A 43-km dark optical fiber link connects Lincoln Laboratory and MIT campus. It was originally deployed as part of a DARPA-funded research project on high-bandwidth optical communications [Ber+02], but was later re-purposed to support quantum networking research and applications.

The Lincoln-MIT campus link is comprised of a pair of optical fibers linking the Group 67 lab in C-448 with Quanta. The optical fibers are comprised mostly of SMF-28 (with some short sections of TruWave) deployed mostly above ground. A schematic of the deployed fiber is shown in Figure 5-1. The one-way loss over this stretch of fiber has previously been measured at 12-15 dB [Gre+17]. Figure 5-2 displays an optical time-domain reflectometer (OTDR) trace of the fiber, which maps the signal loss as a function of distance. The OTDR sends infrared pulses down the fiber and characterizes its loss profile at each point along a signal's path by measuring the signal back reflections. The OTDR is also useful for identifying any break points in the fiber that need repair. It can be observed in the trace that, in addition to the approximately 0.2 dB/km propagation loss, there is significant discrete loss close to the MIT end due to connectors. Previous work has been done to stabilize this link and characterize its one-way noise [Zha+18; Gre+17]. A residual phase noise plot of the fiber generated from that work can be found in Figure 5-3.

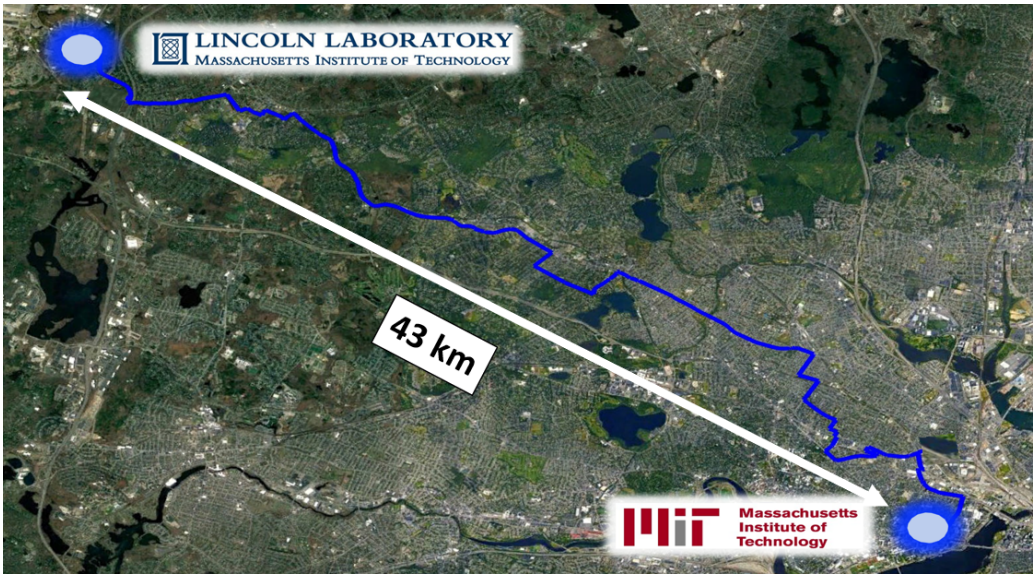

Figure 5-1: Aerial view of the deployed fiber between the Group 67 lab C-448 and MIT Quanta lab. This map is oriented with North pointing up.

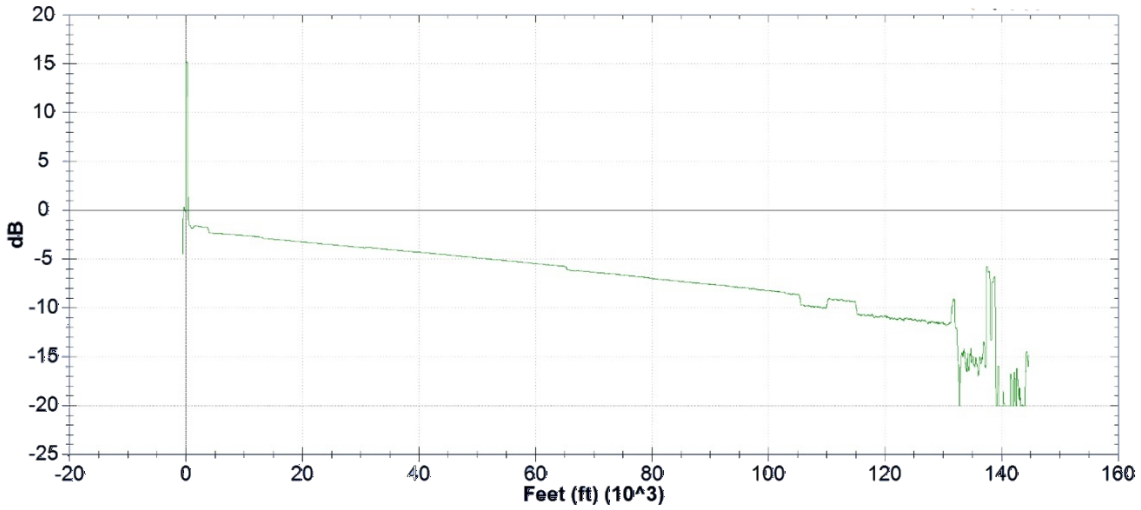

Figure 5-2: Optical time-domain reflectometer trace of the deployed fiber going one-way from Lincoln to MIT. This graph depicts loss as a function of distance for a 1550 nm signal. The vertical line indicates the end of the fiber internal to the OTDR and the start of the deployed fiber. The spike at the end of the trace around 140×10^3 ft (42.6 km) indicates fiber termination. The vertical jumps between 100×10^3 ft (30.5 km) and 120×10^3 ft (36.5 km) are likely places where TruWave fiber has been installed.

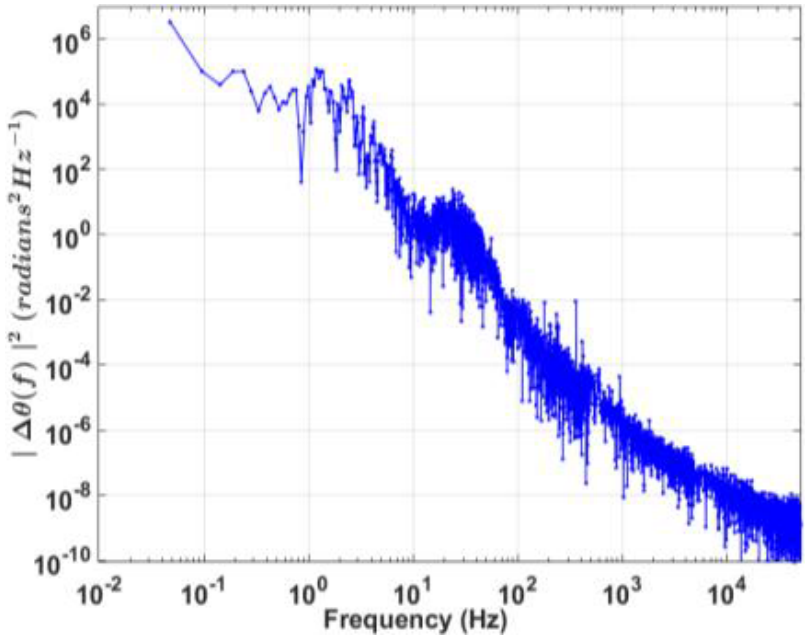

Figure 5-3: Power spectral density of phase noise contributed by the 42 km deployed fiber to an optical signal. This measurement was made as part of fiber stabilization effort in Group 67 [Gre+17].

Quantity	Length	Company	PN (given by company)	Manufacturer
2	450 m	Fiber Instrument Sales	S09SX01CZNPY	Corning
1	450 m	Oz Optics	SMF-633-4/125-3LSZH-L	Nufern

Product Name	Jacket	Termination
SMF-28, Ultra	Yellow, 3mm, plenum rated	Scissor cut
630-HP	Yellow, 3mm, LSZH	Scissor cut

Table 5.1: Manufacturing information about the fiber purchased for installation. The bottom table should be read as a continuation of the top table. LSZH stands for low-smoke zero-halogen.

Type	Core	Cladding	Coating	Coat Material	Temp. Range
SMF-28	8.2 μm	125.0 ± 0.7 μm	242.0 ± 5.0 μm	Acrylate	-60 to 85 °C
630-HP	3.5 μm	125.0 ± 1.0 μm	245.0 ± 15.0 μm	Acrylate	-55 to 85 °C

Table 5.2: Mechanical specifications for each fiber. These numbers can be found on the product sheet for each fiber listed on the manufacturer's website.

5.1.2 The Group 89-Group 67 segment

The link was extended from Group 67 to Group 89 in May 2020. Three 450 m strands of fiber were installed the week of May 18-22, 2020: two SMF-28 strands and one 630-HP strand, detailed in Tables 5.1 and 5.2. The optical characteristics for each fiber are shown in Table 5.3. All of the numbers reported in Tables 5.3 and 5.2 were specified by the manufacturer and do not represent the measured performance of the fibers.

Installation of the fibers was completed by the MIT Lincoln Laboratory Information Services Department (ISD) over the course of three days. The fiber was terminated in the Group 67 laboratory at C-448 and the Group 89 laboratory at L-035A. Figure 5-4 shows an aerial view of

Type	λ Range	Cutoff	Mode Field Diameter	Core Attenuation
SMF-28	1525 - 1575 nm	$\leq$ 1260 nm	10.4 ± 0.5 μm	$\leq$ 0.18 dB/km
630-HP	600 - 770 nm	570 ± 30 nm	4.0 ± 0.5 μm	$\leq$ 12.0 dB/km

Table 5.3: Optical specifications for the 630-HP and SMF-28 fibers at 630 nm and 1550 nm, respectively. These numbers can be found on the product sheet for each fiber listed on the manufacturer's website.

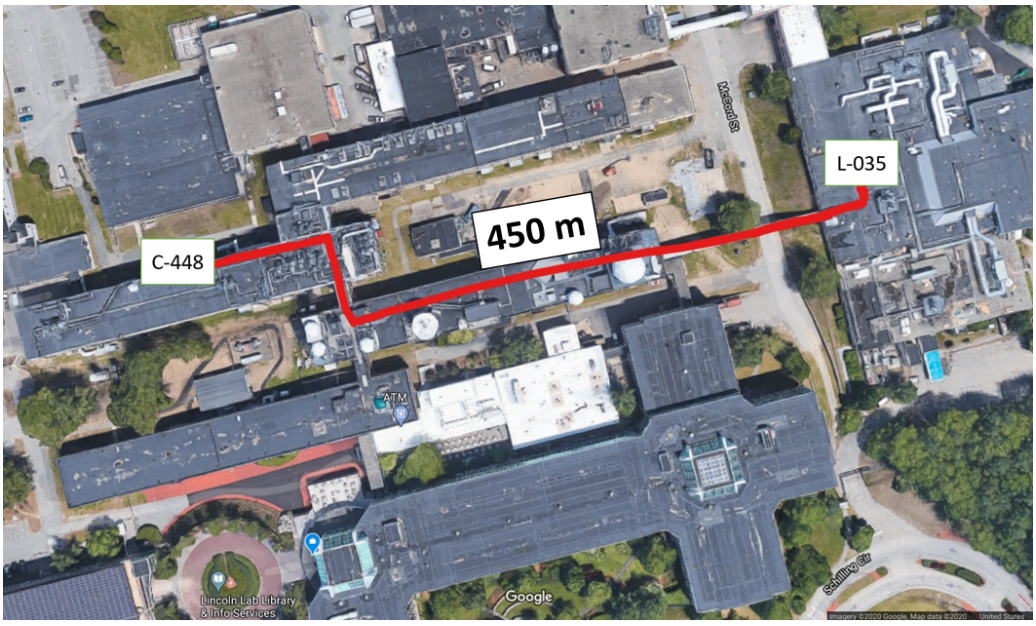

Figure 5-4: Aerial view of the deployed fiber between the Group 67 lab C-448 and Group 89 lab L-035A. This map is oriented with North pointing up.

the fiber path. The SMF-28 strands on the C-448 end of the fiber were terminated with FC/PC connectors, while every other end were terminated with an FC/APC connection.

5.2 Fiber characterization

Understanding the optical fiber characteristics and its influence on transmitted signals is a crucial step in the process of engineering a control system to ameliorate deleterious effects. In this section, we explore some of those characteristics.

5.2.1 Loss

SMF-28 fiber

We measured loss along the SMF-28 strands using an OTDR. Figure 5-5 depicts the loss profile of the SMF-28 cables in round trip configuration (i.e. the ends of the fibers at L-035A were

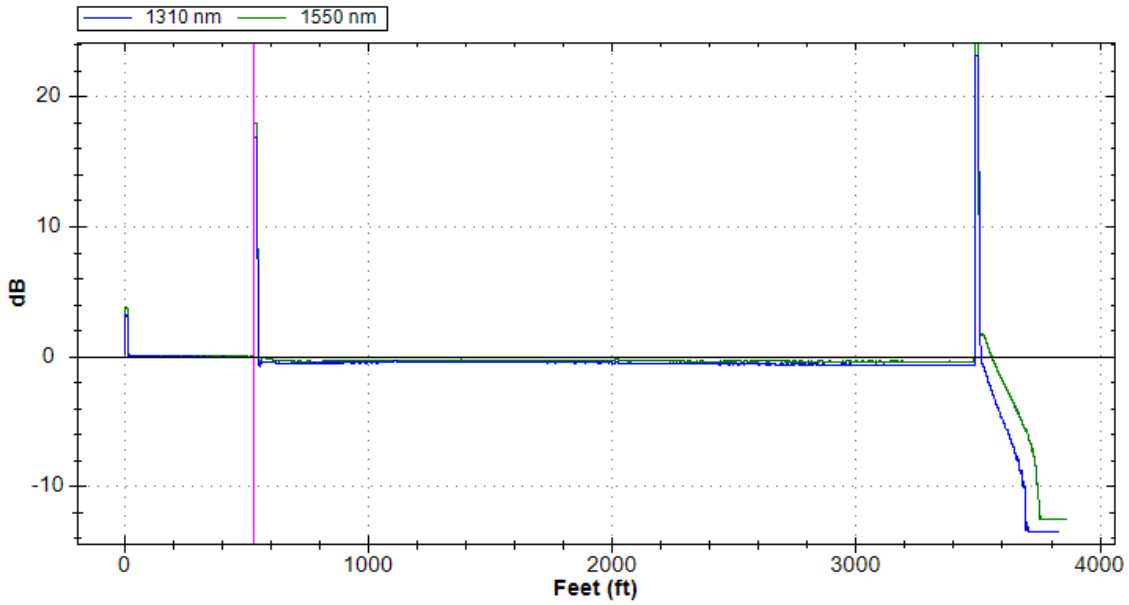

Figure 5-5: Optical time-domain reflectometer (OTDR) trace of the deployed SMF-28 fibers in round trip configuration. This graph depicts loss as a function of distance for 1310 nm and 1550 nm signals. As with Figure 5-2, the vertical line indicates the end of the fiber internal to the OTDR and the start of the deployed fiber and the spike at the end of the trace indicates the fiber termination.

connected to one another). The deployed SMF-28 fiber trace does not begin until 530 ft (161.5 m), where the OTDR fiber connects to it.

The OTDR trace shows no major break points in the deployed fiber, indicating that the SMF-28 installation was successful. The total round trip distance was measured to be 2959 ft (901.9 m). The total loss at 1550 nm along the round trip is 0.42 dB, which includes a 0.3 dB loss from connecting the OTDR to the deployed fiber. This number was validated with a measurement using the Koheras Adjustik (λ = 1549.53 nm). The initial Koheras power entering the fiber was measured at 2.5 mW (3.97 dBm) and its return power was measured at 2.2 mW (3.42 dBm), resulting in a 0.55 dB link loss. Overall, the results indicate that the SMF-28 fibers were manufactured to standard and installed without any issues.

630-HP fiber

Since the OTDR we used (Fluke Networks OptiFiber Pro) only works at IR wavelengths, it could not be used to create a loss profile for the visible 630-HP fiber. Loss along this fiber was measured one way (from L-035A to C-448) using a 650 nm continuous-wave (CW) laser fiber-coupled to the 630-HP fiber. The initial power entering the fiber was measured at P_i = 2.47 mW (3.93 dBm) and its power at the end of the 450 m path was P_{450} = 0.094 mW (-10.3 dBm), which means the total loss was 14.23 dB. To determine how much loss we incurred merely by coupling into the fiber, we also measured the power after the signal traveled through 1 m of 630-HP, which came out to be P_1 = 0.250 mW (-6.02 dBm), meaning that 9.95 dB of the 14.23 dB loss came from coupling. This means the total loss over the 450 m fiber was 4.28 dB (or 9.51 dB/km), which is consistent with the manufacturer's specifications.

5.2.2 Phase noise measurements of the round trip SMF-28 fiber

An optical signal will experience random variations in its phase $\Delta\theta(t)$, known as phase noise, as it travels along a fiber. We measured the phase noise that the fiber imparts on an optical signal using an optical homodyne detection scheme. The experimental setup for the round trip measurement is shown in Figure 5-6. A narrow-linewidth CW laser near 1550 nm is launched into the 900 m fiber and split 50:50 at C-448. One signal (labeled S) travels 900 m to and from L-035A, while the other (labeled L) is tapped locally in C-448. S and L enter a $\frac{\pi}{2}$ optical hybrid device. Inside the $\frac{\pi}{2}$ device, S and L are split once more. One of the L paths is then shifted by $\frac{\pi}{2}$. Both L signals are combined with one of the S signals. After a balanced photodetection, there will be an in-phase and out-of-phase (by $\frac{\pi}{2}$) electrified signal proportional to the $\cos\Delta\theta(t)$ and $\sin\Delta\theta(t)$, respectively. Digitally computing the arctangent directly yields the desired optical phase time series. The benefit of using this method is that our phase noise measurement is insensitive to changes in signal power (i.e. amplitude noise).

The 1550 nm laser used was a narrow-linewidth Koheras Adjustik (λ = 1549.53 nm, P = 2 mW), whose estimated coherence length is longer than the the round trip length of the fibers. The complete parts lists can be found in Table 5.4. The digital sampling oscilloscope records a 24 Gigasample snapshot of in-phase and quadrature voltages over 960 ms, giving a rate of 25 GS/s, which is well above the Nyquist range for the fiber noise we expect based on previous measurements [Gre+17]. Figure 5-7 is a plot of the normalized in-phase and out-of-phase signals.

Qty	Item	Manufacturer	Product #
1	$\frac{\pi}{2}$ optical hybrid	Optoplex	HB-CoAFCS001
1	Balanced detector (350 MHz)	Thorlabs	PDB430C
1	Balanced detector (350 MHz)	Thorlabs	PDB130C
1	Oscilloscope	LeCroy	7300A

Table 5.4: Parts list for the round trip phase noise measurement along the pair of SMF-28 fiber strands.

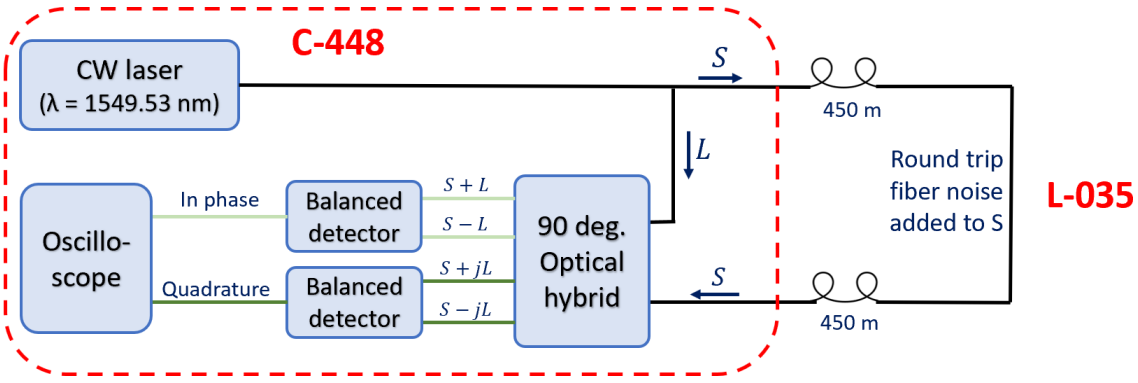

Figure 5-6: Experimental setup to measure the round trip noise for the SMF-28 fibers.

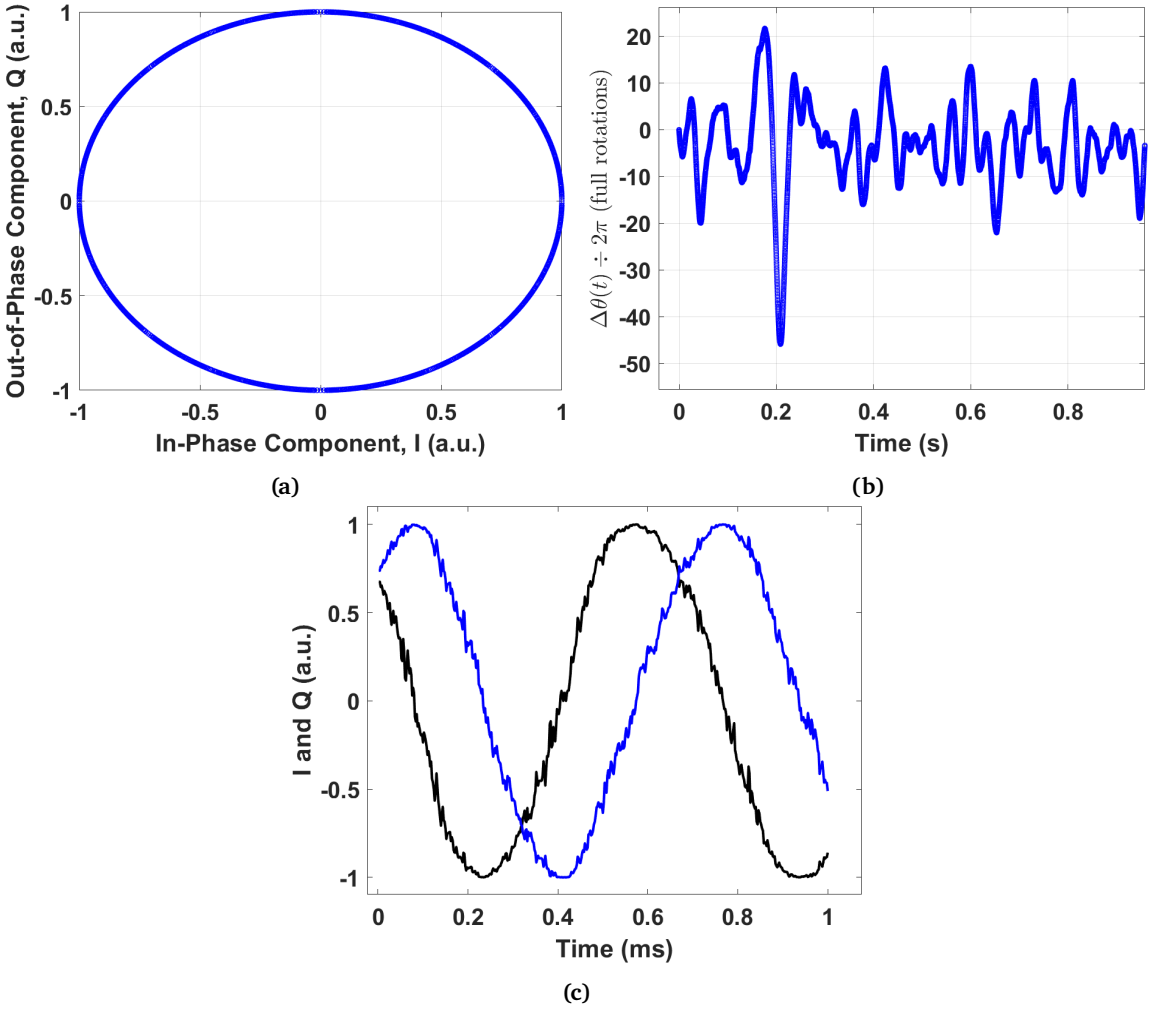

Figure 5-7: **(a)** Phase plot of the fiber noise, normalized; **(b)** Phase noise versus time in a 1-second capture period; and **(c)** In-phase and quadrature signals over time. The signals should be separated by a phase of $\frac{\pi}{2}$ and the sum of their squares should equal 1.

The power spectrum of the optical phase noise was computed from the time series, shown in Figure 5-8. The spectrum revealed a power law characteristic with order f^{-4} up to 1 kHz, f^{-2} from 1 kHz to 10 kHz, and f^{-1} from 10 kHz to 200 kHz, similar to the noise measured over the 43-km segment shown in Figure 5-3.

One artifact from the experiment worth noting is that the fiber noise decreases significantly until it reaches the system noise floor from 10 kHz to 20 kHz. Our initial thoughts were that this may be due to the bandwidth of one of the electronic components in the measurement scheme such as the balanced detectors or oscilloscope. But a closer inspection of each RF component indicates that they each have a bandwidth well over 20 kHz. This steep drop was consistent across multiple measurements taken at different times throughout the day. Its presence merits further investigation.

Phase noise in this link can be reduced by using active noise cancellation. In previous work, it was shown that actuation with a low-bandwidth piezo fiber stretcher and a high-bandwidth electro-optical phase modulator with a second-order analog phase-locked loop was highly effective in reducing the variance of the fiber-induced phase noise, σ_{pn}^2, to less than 0.01 rad^2 with a servo bandwidth of 250 kHz [Ste16]. Since the fiber noise of the 450 m and 42 km link are the same order of magnitude, it is reasonable to assume that a 250 kHz loop bandwidth would also be suitable for noise compensation over the 450 m stand.

5.2.3 Polarization stability of the round trip SMF-28 fiber

The output polarization for transmitted light over non-polarization-maintaining single-mode fiber will be time varying and not identical to the light's input polarization. The setup for measuring polarization noise over the round trip of the SMF-28 fiber is depicted in Figure 5-9 and the results of this measurement are plotted in Figure 5-10. The light from a 1550 nm CW laser is polarization-stabilized and then its Stokes parameters over time are recorded using a polarimeter. The same signal then travels the round trip path of the deployed fiber and the same measurement is conducted. Comparing the two results will indicate the polarization noise contributed by the fiber. The CW laser used was a Koheras Adjustik (λ = 1549.53 nm, P = 2 mW), the polarization stabilizer was a General Photonics POS-103A, and the polarimeter was a General Photonics PSY-101. The results indicate that the noise added by the fiber on the day the measurement took place did not change the angle of polarization for the signal more than 0.06 rad in any direction.

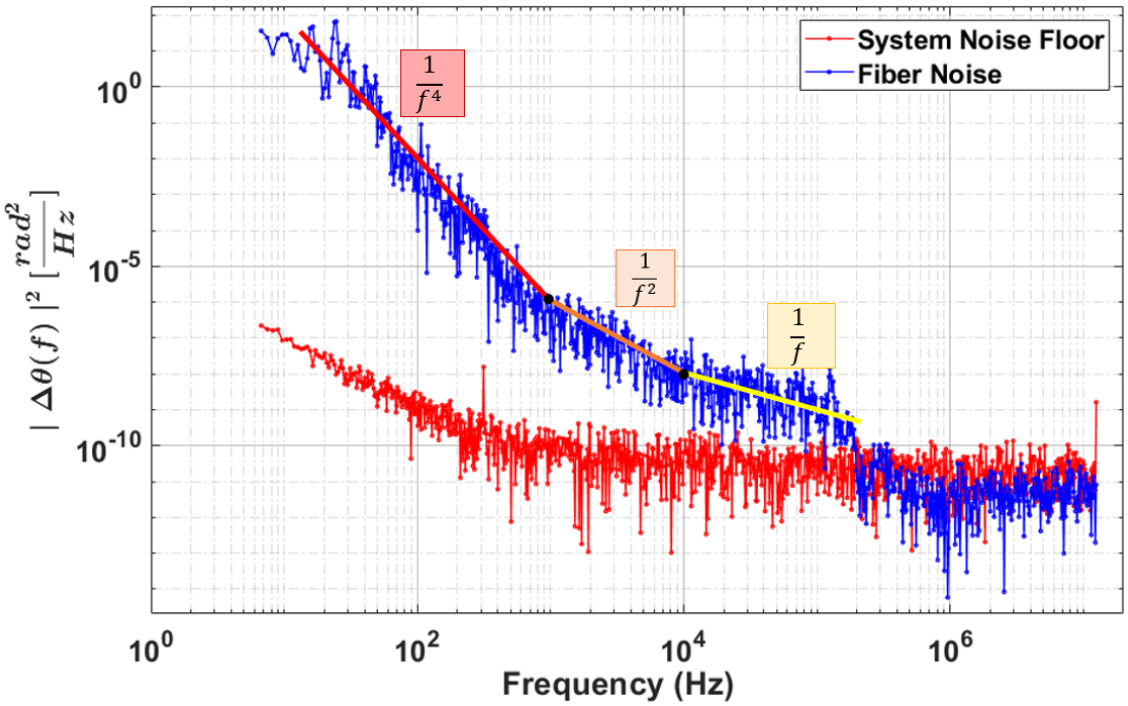

Figure 5-8: Power spectral density of the phase noise contributed by the deployed fiber to the signal under test with super-imposed power law "guides to the eye." The noise floor of the system was measured by beating the laser with itself locally.

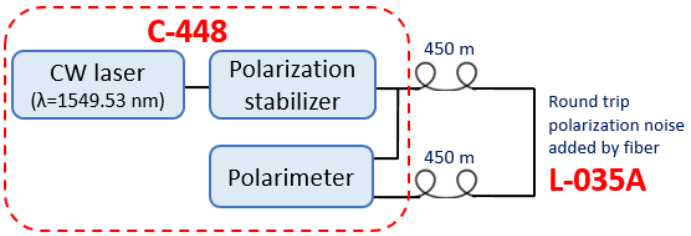

Figure 5-9: Setup for measuring the polarization noise of the 900 m round trip SMF-28 path.

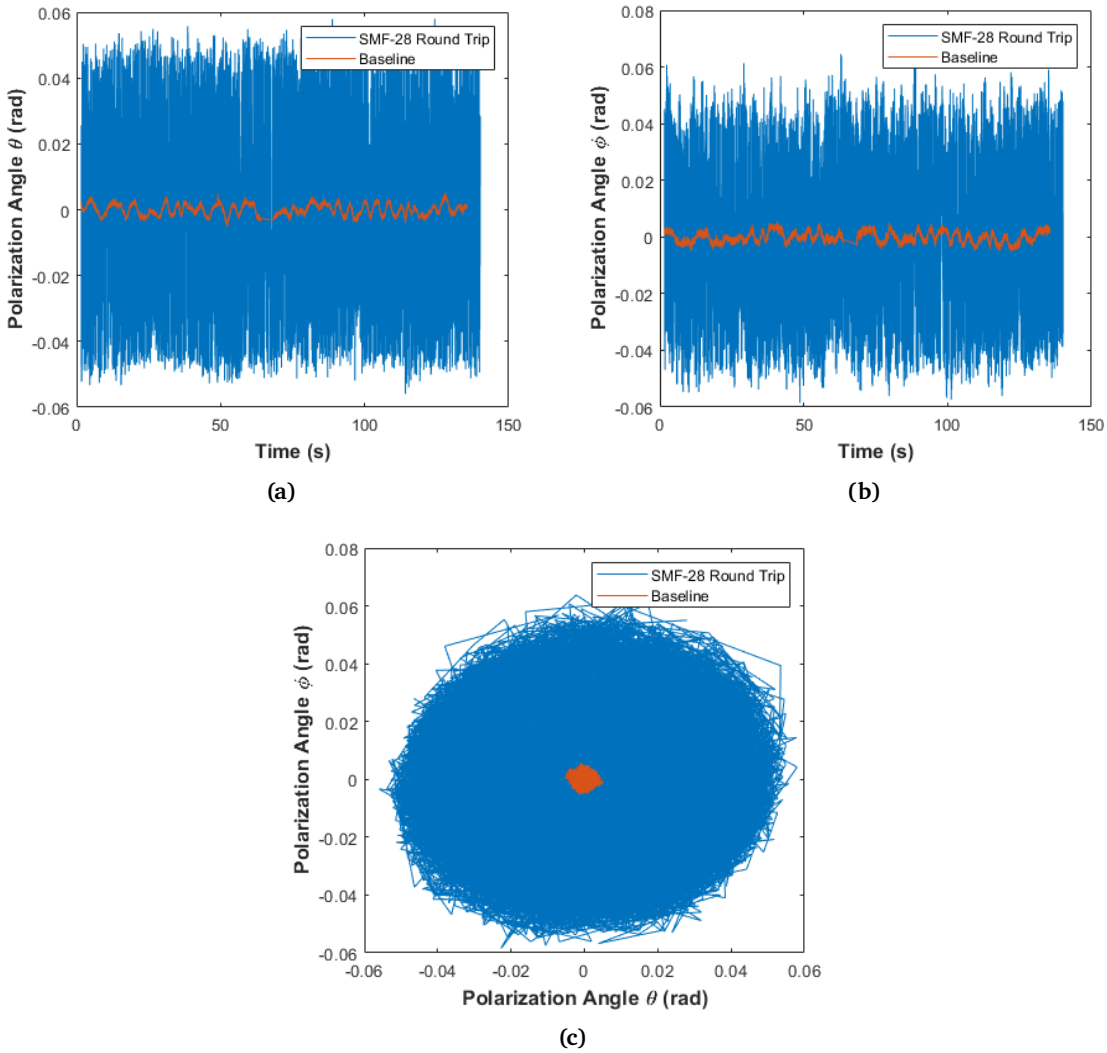

Figure 5-10: Polarization noise over the local path (dubbed "baseline") and the 900 m round trip of the SMF-28 fiber. θ and ϕ are the detrended polarization angles of the light in spherical coordinates. The average degree of polarization (DOP) for the baseline measurement is 0.9847, while the average DOP after traveling through the fiber is 0.9963.

Qty	Item	Manufacturer	Product #
1	$\frac{\pi}{2}$ optical hybrid	Optoplex	HB-CoAFCS001
1	Balanced detector (350 MHz)	Thorlabs	PDB430C
1	Balanced detector (350 MHz)	Thorlabs	PDB130C
1	Oscilloscope	LeCroy	7300A
1	Faraday mirror	Thorlabs	MFI-1550-FC
1	Fiber-coupled polarization splitter	Thorlabs	PFC1550F

Table 5.5: Parts list for the double pass phase noise measurement on each SMF-28 strand.

5.3 Future link stabilization work

We were not able to complete every single test previously planned. The remaining experiments planned were:

- Phase noise measurement of the all fiber strands in a double pass configuration.
- One-way polarization noise over the 630-HP fiber.
- Changes in fiber length throughout the day by measuring pulse time-of-flight.
- Phase noise stabilization via acousto-optic modulator (AOM) with a feedback loop.

In this section, we discuss some of these experiments in greater detail.

5.3.1 Double pass phase noise measurement

If we want to characterize the phase noise for only a single strand of fiber, we can do so in a double pass configuration. The setup for doing a double-pass measurement in the telecommunications wavelength range is shown in Figure 5-11. As with the round trip phase noise measurement described in Section 5.2.2, we use the narrow-linewidth Koheras Adjustik (λ = 1549.53 nm) because its coherence length is longer than that of the signal path. The principal for measuring this value is the same as in the round trip case, with the exception of the path that S takes. We control the polarization of the original 1550 nm signal before it is split. S travels down the SMF-28 fiber and is reflected off of a Faraday mirror, which rotates all polarization states in the signal by $\frac{\pi}{2}$. This allows us to use a polarization splitter to separate the signal that travels the entire 900 m from any back reflections that may corrupt the measurement. A nominal parts list for this experiment at 1550 nm can be found in Table 5.5.

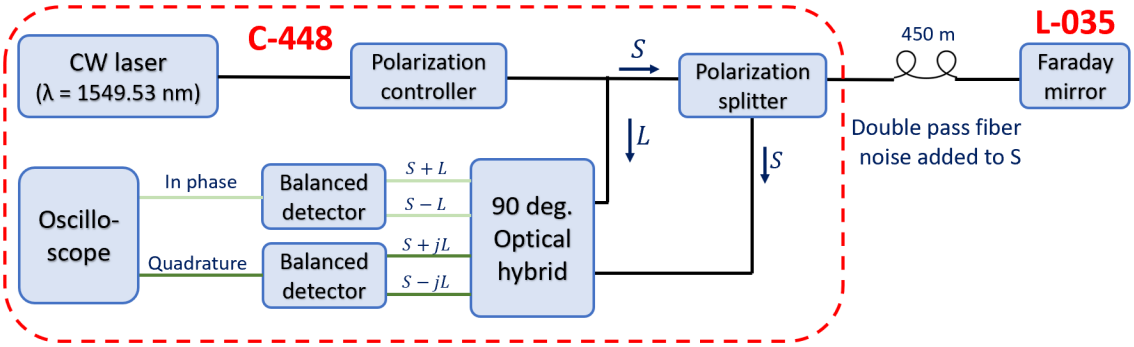

Figure 5-11: Experimental setup to measure the double pass phase noise for each SMF-28 fiber.

5.3.2 Changes in fiber length

We would like to see how the length of the fiber changed due to temperature fluctuations over the course of a day. The coefficient for linear thermal expansion for glass is on the order of 10^{-6} m/(m°C). The round trip fiber length is approximately 1 km, so we expect to see a 1 mm change in the fiber length per 1°C change in temperature, which is beyond the resolution capabilities of the OTDR.

Instead, we can set up an experiment to measure the change in a pulse's time-of-flight (TOF) through the fiber, as shown in Figure 5-12. The pulsed laser is split into a local path, which stays within the lab, and a signal path, which travels across the fiber. The pulse train from each path is detected with a high-bandwidth photodetector and is recorded using a time tagger with ps-level resolution.

A pulse travels through fiber at approximately 2×10^8 m/s, which means a 1 mm change in path length will manifest as a 5 ps change in relative arrival time between the two pulses being detected. The PicoHarp 300 can resolve arrival times down to 4 ps in precision, so it is suitable for measuring the change in pulse TOF due to temperature changes over the course of a day. The PicoHarp is not well-suited for recording time stamps of 10 MHz pulses because they arrive too quickly. Instead of using a modelocked laser, we can carve out pulses at a kHz rate using a 1550 nm CW laser, an electro-optic modulator, and a pattern generator.

Another way to achieve this measurement is by having two time-taggers synced to the same clock reference. Unfortunately, this would require a shared clock with ps-level stability, which

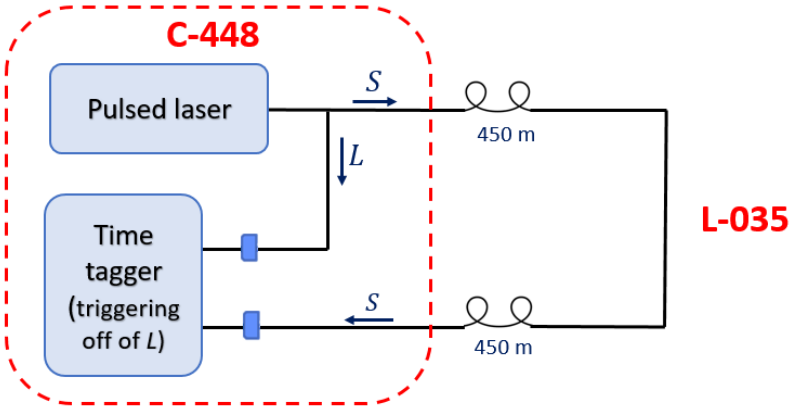

Figure 5-12: Experimental setup to measure the change in time of flight for a signal over the deployed fiber.

does not exist commercially. This highlights another example of how a global quantum clock network could enable new methods for conducting scientific experiments, as discussed in Section 1.2.2.

5.3.3 Phase noise stabilization over long-distance single-mode fiber

Previous work in Group 89 and Quanta has been done on compensating for fiber-induced phase noise over short lengths of polarization-maintaining (PM) fiber at visible wavelengths, employing a homodyne detection scheme with an error signal that is fed back into an AOM. While this scheme may also be suitable over longer, non-PM fiber at infrared wavelengths, work done by other groups [Dro+14; Cal+14] suggests that a second AOM will be required to reduce the impact of back reflections. Figure 5-13 is diagram of the scheme. The -1 order AOM signal travels down the fiber and is reflected back, where it is beat with the +1 AOM signal (that is kept locally) on a photodetector. This generates a feedback signal that can be used to modify the driving frequency of the AOM.

Figure 5-13 also contains two additional modifications to the original design. First, to minimize issues regarding polarization noise along the single mode fiber, the feedback signal can be reflected off of a Faraday mirror that rotates every polarization state in the signal by $\frac{\pi}{2}$, so that the polarization states of the feedback local signals are orthogonal when they are detected. Second, to ensure the feedback signal we are using traveled down the entire length of the fiber

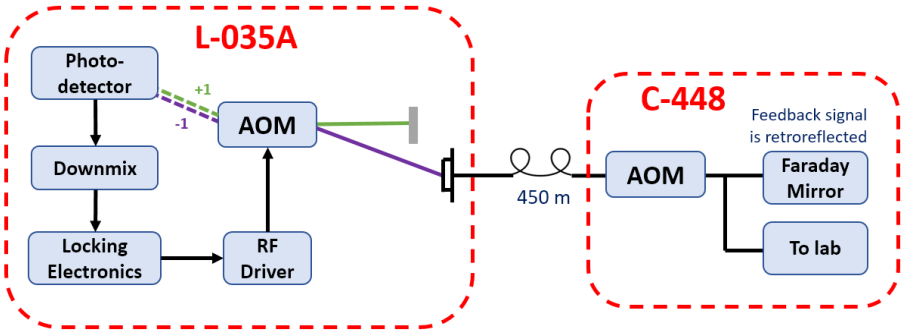

Figure 5-13: Setup for cancelling one-way fiber noise using an AOM.

and is not back reflections, the frequency of the light can be shifted again at the very end of the path before it hits the Faraday mirror.

5.3.4 Other technical challenges and future work

We may need to develop a method for noiseless frequency transfer between visible and IR wavelengths when interfacing with other quantum systems. As shown in our loss measurement over the 450 m strands, visible fiber experiences significant loss over long distances, unlike telecommunications fiber which is more suitable for long distance transport of quantum signals. Since we are concerned with reducing aspects of channel noise wherever possible, we should also be concerned with the noise induced by frequency conversion. Additionally, if we want to have multiple wavelengths interact with one another, it may helpful if they were stable relative to one another. This is where we can leverage the power of a frequency comb.

A frequency comb is a useful tool for building a quantum network because it is essentially a very precise ruler (less than 100 mrad in phase noise [Tre+19]) in the frequency domain. Its comb lines can be used to measure the absolute frequency of a signal and lock one signal to another in a noiseless fashion at nearly any wavelength from 600 nm to 2000 nm. Frequency combs can also be compared with one another for characterizing the properties of a channel, such as one-way fiber noise, as demonstrated by Zhang et al. [Zha+18]. Understanding how to use a frequency comb and interface it with other devices may become important in building a stable quantum link.

Aside from the channel characterization and stabilization projects mentioned in Section 5.3,

we would like to achieve a narrow linewidth transfer of 674 nm light from Group 89 to Quanta. This could involve using a frequency comb for converting the light to a telecommunication wavelength for transport over the 42 km fiber. Once this has been demonstrated, the 674 nm laser at Lincoln can be used to control an ion trap at MIT from a distance. In the future, we could use this link to establish a two-way communication protocol for quantum clock synchronization [Chuoo] to enable some of the applications discussed in Section 1.2.2. In the end, both laboratories could gain access to a stable clock signal to be used for future experiments.

5.4 Conclusion

In this chapter, we presented characterization work on the Group 89-Group 67 segment of the 43 km fiber link connecting Lincoln to MIT. Understanding how the fiber affects classical and quantum signals alike can potentially help develop engineering solutions for building a stable quantum link between Group 89 and Quanta. What is learned about link stabilization from this project may prove useful in establishing other long-distance quantum links, such as the quantum link proposed in Chapter 4.

Chapter 6

Conclusion

We began this thesis in Chapter 1 by exploring how quantum networking will likely be a disruptive technology, offering more than just the promise of key distribution free from eavesdropping, as discussed in Section 1.2. In Section 1.3, we established why international cooperation could be useful in building a quantum network by delving into some of the challenges associated with scaling beyond a couple nodes. Although this analysis was not scientifically comprehensive, it helped inform the policy discussions in Chapters 2 and 3.

To consider the feasibility of cooperation between the U.S. and China, in Chapter 2 we examined what forces dictate QIS research in each country by creating a stakeholder framework, described in Section 2.2. We show that the government-technologist partnership, which we argue is what primarily dictates international scientific cooperation, is unified in the QIS research landscape for both the U.S. (Section 2.3) and China (Section 2.4).

In Section 3.1, we argued that the U.S.-China relationship has reached its lowest point in history in 2020. We then discussed how this has resulted in the U.S. adopting an increasingly restrictive policy regarding scientific collaboration with China (Section 3.1.3). We argue that innovation has become intertwined with modern diplomacy. Therefore, any proposal for a joint quantum networking project would be mired in the urgent geopolitical crisis created by the U.S. and China. So, in Section 3.3, we considered how a joint quantum project could afford us the opportunity to strengthen bilateral stability with China, which we argue could be pivotal in addressing several security challenges the U.S. currently faces (Section 3.2).

We believe that the U.S.-China relationship is at a turning point; the next steps that either country takes may have decades-long consequences for global stability. Although we contend that a joint quantum project could be symbolically powerful (Section 3.3.1), there are still strategic (Section 3.3.2) and intelligence (Section 4.4) risks which may need to be addressed in choosing to pursue a joint quantum project. In Chapter 4, we presented a framework for quantum network collaboration that might be a good starting point: a joint project on sharing entanglement between the U.S. and China. This could serve as the foundation for future cooperation in quantum information science and could send a signal to the rest of the world that each country is interest in promoting stability. Finally, in Chapter 5, we presented characterization work on the 43 km optical fiber link connecting MIT to Lincoln. This work may help better understand some of the technical challenges associated with building a bilateral quantum link, such as the one proposed in Chapter 4.

Appendix A

Code

This appendix is a repository of some programs that I wrote or helped write during my research that may be of future use to Group 67.

A.1 Determining Doppler Shift for Mode Locked Laser in LEO

```
%% Tracking Doppler of a Satellite

% The purpose of this program is to determine the rate of change of a
% Doppler shift for a satellite passing overhead. This will inform whether
% or not a laser has the range to adjust its cavity for Doppler.

clear all;clc;

c = 3e5; %speed of light [km/s]
v = 7.823; %speed of aircraft [km/s]
t = linspace(-60,60,10000); %time vector [s]
f_0 = 1e9; %rep rate of laser [Hz]
h_min = 300; %max satellite altitude [km]
h_max = 500; %min satellite altitude [km]
x = abs(v.*t); %distance from satellite to observer (ground trace) [km]

for h=h_min:10:h_max
    phi = atan(h./x); %angle between observer and satellite
```

```
    del_v = v*cos(phi); %relative velocity
    del_f = del_v/c*f_o; %doppler shift

   % Change in doppler shift over time
    ddelf_dt = gradient(del_f)./gradient(t);
    plot(t,abs(1e-3.*ddelf_dt))
    hold on
end

ylabel('Magnitude of d/dt \Deltaf [kHz/s]')
xlabel('Time [s]')
title('1GHz Laser Doppler Shift Change for Overhead Satellite')
grid on
figure;

for h=h_min:10:h_max
    phi = atan(h./x); %angle between observer and satellite
    del_v = v*cos(phi); %relative velocity
    del_f = del_v/c*f_o; %doppler shift

    plot(t,1e-3.*del_f)
    hold on
end
ylabel('Magnitude of \Deltaf [kHz]')
xlabel('Time [s]')
title('1GHz Laser Doppler Shift for Overhead Satellite')
```

A.2 Determining Pulse Width After Filtering

```
%% Mixing and Matching Koshin Filters

% The purpose of this program is to determine different filters we might use
% in order to broaden a 200 fs pulse to 1 ps.
% Author: Nolan Hedglin, Group 67

% Input: 3,6,10,20,30 dB bandwidths of filters; laser spectrum
% Output: pulse spectrum, power

%% Parameters you might be interested in modifying can be found:
% serial number of filter: line 65
```

```
% center wavelength of filter: line 66
clc; clear all; close all;

%% Input parameters

lambda = 1530:0.1:1570; % Wavelength vector [nm]
freq = (1e-12*3e8)./(lambda.*1e-9); % Frequency [THz]
t = -400:2:400; % Time vector [fs]
f_rep = 1e9; % Repetition Rate [Hz]

% Scaled time vector to match pulse shapes after fourier transform. Just
% gonna have to trust that this is important for scaling purposes.
t_scaled = -16000:80:16000; % unitless

FWHM = 14; % FWHM of the laser [nm]
tau = 185; % Temporal pulse width [fs]
P_peak = 0.4; % Peak power of pulse [kW]
duty_cycle = tau*(1e-15)*f_rep; % Duty cycle of laser
P_ave = P_peak*(1e6)*duty_cycle; % Average power of laser [mW]

% Define  pulse shape (sech^2)
spectrum_laser = sech((lambda-1550)/(FWHM/1.76)).^2; % Spectral shape of pulse
time_laser = P_peak*sech(t/(tau/1.76)).^2; % Temporal shape of pulse

% Define koshin filters and their spectra
KoshinList = readtable('Koshin_Master_List.csv'); % Read in the Koshin master list
SN = KoshinList.SN; % SN list of filters


% Create a table to store filter data for retrieval. I define a table,
% convert it to a cell array, populate its fields, then convert back into a
% table. I hate this.
filter_data = table2cell(table('Size',[length(SN) 2],'VariableTypes',{'single','
    cell'},...
    'VariableNames',{'SN','BW'}));

for i = 1:length(SN)
    filter_data{i,1} = SN(i);
    filter_data{i,2} = [0 -1 ; -KoshinList.three_dB(KoshinList.SN == SN(i))/2 -3
    ;...
        KoshinList.three_dB(KoshinList.SN == SN(i))/2 -3 ; ...
```

```
        -KoshinList.six_dB(KoshinList.SN == SN(i))/2 -6 ;...
        KoshinList.six_dB(KoshinList.SN == SN(i))/2 -6 ;...
        -KoshinList.ten_dB(KoshinList.SN == SN(i))/2 -10 ;...
        KoshinList.ten_dB(KoshinList.SN == SN(i))/2 -10 ;...
        -KoshinList.twenty_dB(KoshinList.SN == SN(i))/2 -20 ;...
        KoshinList.twenty_dB(KoshinList.SN == SN(i))/2 -20 ;...
        -KoshinList.thirty_dB(KoshinList.SN == SN(i))/2 -30 ;...
        KoshinList.thirty_dB(KoshinList.SN == SN(i))/2 -30 ;...
        -KoshinList.thirty_dB(KoshinList.SN == SN(i))/2-8 -40 ;...
        KoshinList.thirty_dB(KoshinList.SN == SN(i))/2+8 -40;...
        -KoshinList.thirty_dB(KoshinList.SN == SN(i))/2-15 -40 ;...
        KoshinList.thirty_dB(KoshinList.SN == SN(i))/2+15 -40];
end
filters = cell2table(filter_data,'VariableNames',{'SN','data'}); % back to table
    form

% It should be noted that I created fake 40dB and 50dB BW data points in
% order to make the curve fitting process more natural for gaussian shaped
% filters. This means that the fit function for filters 1426-1428 (which
% are not gaussian) will look strange. Need to record more data points at
% 40dB and 50dB next time if needed.

%% Select the filters you want to test
ser_num = 1953; % enter the serial number of the filter you want to test
filter_CW = 1550; % center wavelength for the filter

prefit_filter = filters.data{SN == ser_num}; % retrieving data from table for
    filter
filter = fit(prefit_filter(:,1),prefit_filter(:,2),'smoothingspline'); % fit a
    function to the data

% filter is now a fitted function that we can sample from
filter_spectrum = 10.^(filter(lambda-filter_CW)/10);

%% Filtering

% Convolve filter and spectra (pick any combo)
filtered_pulse = spectrum_laser.*filter_spectrum.';

% Inverse Fourier transform of filtered spectrum to get temporal pulse
filtered_temporal = (1/2.5).*fftshift(ifft(filtered_pulse,length(t)));
```

```
%unfiltered_temporal = (1/4).*fftshift(ifft(spectrum_laser,length(t)));

%% Results
% Plot filter spectrum in dB so it looks normal
plot(filter)
title('Filter Spectrum in dB')
xlabel('Distance from filter peak [nm]')
ylabel('Extinction [dB]')
figure;

%% Now normalize it
% plot(lambda,filter_spectrum)
% title('Normalized Filter Spectrum')
% figure;

% Plot filtered pulse spectrum
yyaxis right
plot(lambda,filter_spectrum)
title('Pulse Spectrum')
hold on

yyaxis left
semilogy(lambda,spectrum_laser)
hold on
semilogy(lambda,filtered_pulse)
legend('Before Filtering','After Filtering','Filter')
ylabel('Power Spectrum [arb.]')
xlabel('Wavelength [nm]')
grid on
figure;

% Calculate FWHM of new pulse shape
filtered_fit = fit(t_scaled.',abs(filtered_temporal.'),'smoothingspline');

P_peak_new = filtered_fit(0); % peak power of filtered pulse

% Finding indices of all elements whose difference with half max of array
% is within tolerance.
y = find(abs(abs(filtered_temporal)-P_peak_new/2) < 0.001);
tau_new = abs(2*t_scaled(y(round(length(y)/4)))); % 2*value at half max = FWHM [fs
    ]
```

```
129
130 % Compute the new average power
131 duty_cycle_new = tau_new*(1e-15)*f_rep; % Duty cycle for filtered pulse
132 P_ave_new = P_peak_new*(1e6)*duty_cycle_new;
133
134 % Plot temporal shape of filtered pulse with unfiltered pulse
135 yyaxis right
136 plot(t_scaled,abs(filtered_temporal))
137 title('Pulse propagation in time')
138 hold on
139 yyaxis left
140 plot(t,time_laser)
141 ylabel('Power [kW]')
142 xlabel('Time [fs]')
143 grid on
144 xlim([-1500,1500])
145 legendLabel{1} = ['Unfiltered Pulse: FWHM =',num2str(tau),...
146     ' fs, Power = ',num2str(P_ave), ' mW'];
147 legendLabel{2} = ['Filtered Pulse: FWHM =',num2str(tau_new),...
148     ' fs, Power = ',num2str(P_ave_new), ' mW'];
149 legend(legendLabel);
150 % hold on
151 % plot(t_scaled,abs(unfiltered_temporal))
```

A.3 Calculating Root-Mean Squared Jitter from a Phase Noise Analyzer

```
1  function BasebandPhaseNoiseAnalysis_190523_3
2  %BaseBandPhaseNoiseAnalysis_190523 Process data from E5052.
3
4  % Get Key File data.
5  keyData = readtable('key.csv');
6
7  % Get data file names and sort.
8  [fileList, fileListNumber] = getFiles;
9
10 for n = 1:numel(fileList)
11     AnalysisType = keyData.Type{n};
12     filename = fileList{n};
13     nIndex = keyData.Number == fileListNumber(n);
```

```
    carrierFrequency = keyData.Carrier_MHz(nIndex) * 1e6; % Hz
    refVoltage = keyData.RefVoltage_V(nIndex);
    [freq{n}, amp{n}, jitter(n)] = getDataCalculateJitter(...
        filename, refVoltage, carrierFrequency, AnalysisType);
    if fileListNumber(n) < 10
        spacerOption = ' ';
    elseif fileListNumber(n) >= 10
        spacerOption = '';
    end
    legendLabel{n} = [...
        'File', fileList{n}(1:end-4), ...
        ' ', spacerOption, '\sigma_j=', num2str(round(jitter(n)*1e12,2)), ...
        'ps ', ...
        keyData.Description{nIndex}...
        ];
end

% Plot
figure
for n = 1:numel(fileList)
    switch AnalysisType
        case 'Baseband'
            semilogx(freq{n}, amp{n})
        case 'Carrier'
            loglog(freq{n}, amp{n})
    end
    if n == 1
        hold on
    end
end
leg = legend(legendLabel, 'location', 'best');
leg.ItemHitFcn = @hideShowLine;
xlabel('Frequency [Hz]')
ylabel('Phase Noise [dBc/Hz]')
title('Jitter Measurement')
grid on
set(gca,'fontsize',16, 'fontweight', 'bold')
end

function [fileList, fileListNumber] = getFiles
%getFiles Subfunction to bring in the list of data files.
```

```
%   Detailed explanation goes here

dirName = cd;
dirData = dir(dirName);      % Get the data for the current directory
dirIndex = [dirData.isdir];  % Find the index for directories
fileList = {dirData(~dirIndex).name}';  % Get a list of the files
fileListFindCSV = strfind(fileList,'.csv');
csvIndex = true(numel(fileList),1);
for n = 1:numel(fileList)
    if isempty(strfind(fileList{n},'.csv')) || ~isempty(strfind(fileList{n},'key.csv'))
        csvIndex(n) = false;
    end
end
fileList(~csvIndex)=[];
fileListNumber = zeros(numel(fileList),1);
for n = 1:numel(fileList)
    fileListNumber(n) = str2double(fileList{n}(1:end-4));
end
[fileListNumberSort, fileListNumberSortIndex] = sort(fileListNumber);
fileList = fileList(fileListNumberSortIndex);
fileListNumber = fileListNumberSort;

end

function [ f, L_dBc, J ] = getDataCalculateJitter( filename, refVoltage, carrierFrequency,
    AnalysisType )

%getDataCalculateJitter Subfunction to get data and calculate jitter.
%   Detailed explanation goes here

switch AnalysisType
    case 'Baseband'
    case 'Carrier'
end

% Get data from file.
data = csvread(filename,1);
f = data(:,1);
switch AnalysisType
```

```
94      case 'Baseband'
95          L_dBV = data(:,2);
96          Vo_peak = refVoltage;
97          Vo_rms = Vo_peak/sqrt(2);
98          alpha = (pi/2)/Vo_rms;
99          L_dBc = 10*log10( alpha * 10.^( L_dBV/10 ) );
100     case 'Carrier'
101         L_dBc = data(:,2);
102 end
103
104 % Calculate Integral Phase Noise
105 % Calculate phase noise: Approximate phase noise with trapazoidal function
106 % and integrate from o to the Nyquist frequency
107 freqNyquist = ceil(carrierFrequency/2); % integrate only to Nyquist Freq.
108 fNyquistIdx = f < freqNyquist;
109 % fNyquistIdx = true(size(f)); % uncomment this line to integrate all data
110 f_integrate = f(fNyquistIdx);
111 L_dBc_Integrate = L_dBc(fNyquistIdx);
112 L_Integrate = 10.^( L_dBc_Integrate/10 );
113 I_radians = trapz(f_integrate, L_Integrate);
114 I_dBc = 10 * log10( I_radians );
115
116 % Calculate RMS Noise
117 N = sqrt( 2 * 10 .^ (I_dBc/10) ); % radians
118
119 % Calculate RMS Jitter
120 J = N / (2 * pi * carrierFrequency); % seconds
121
122 % Display the calculated jitter to the command line
123 fprintf('jitter = %f ps \n', J*1e12)
124
125 end
126
127 function hideShowLine(src,event)
128 %hideShowLine Subfunction for plotting with clickable legend.
129 %   This callback toggles the visibility of the line
130
131 if strcmp(event.Peer.Visible,'on')   % If current line is visible
132     event.Peer.Visible = 'off';      %   Set the visibility to 'off'
133 else                                 % Else
134     event.Peer.Visible = 'on';       %   Set the visibility to 'on'
```

```
end

end

% function blinkLine(src,event)
%%blinkLine Subfunction for plotting with clickable legend.
%%  This callback causes the line to "blink"
%
% for id = 1:3                          % Repeat 3 times
%     event.Peer.LineWidth = 3;         % Set line width to 3
%     pause(0.2)                        % Pause 0.2 seconds
%     event.Peer.LineWidth = 0.5;       % Set line width to 0.5
%     pause(0.2)                        % Pause 0.2 seconds
% end
%
% end
```

A.4 Plotting Polarization Noise over the Fiber Link

```
% This program reads in a file that records the stokes parameters from a
% polarimeter and plots polarization on the Poincare sphere. So is the
% intensity and S1-3 are the cartesian coordinates of polarization.

% Author: Nolan Hedglin (GR67) - 7/2/2020

clear all

%% Read in the polarization data

filename1='C:\Users\NO28631\Documents\Polarization Noise\
    Baseline_1550nm_1ms_sample_interval.csv';
filename2='C:\Users\NO28631\Documents\Polarization Noise\RT_SMF28_1ms_Po=2mW_P1
    =0-08mW.csv';

Stokes1 = readmatrix(filename1); %Matrix that contains time, so-3, and degree of
                        %polarization (DOP, normalized)
Stokes2 = readmatrix(filename2);

t1 = Stokes1(:,1); % time vector (ms)
s1o = Stokes1(:,2); % so (power)
```

```
s11 = Stokes1(:,3); % s1 (stokes parameter)
s12 = Stokes1(:,4); % s2
s13 = Stokes1(:,5); % s3
DOP1 = Stokes1(:,6); % degree of polarization, normalized

t2 = Stokes2(:,1); % time vector (ms)
s20 = Stokes2(:,2); % so (power)
s21 = Stokes2(:,3); % s1 (stokes parameter)
s22 = Stokes2(:,4); % s2
s23 = Stokes2(:,5); % s3
DOP2 = Stokes2(:,6); % degree of polarization, normalized

%% Convert polarization to spherical coordinates

% p = sqrt(s1.^2 + s2.^2 + s3.^2)./so; %another way to calculate DOP (not
                                       %normalized)

r1 = s10.*DOP1; %length of polarization vector from origin
theta1 = atan(s12./s11); %angle from x axis
phi1 = pi/2 - atan(s13./sqrt(s11.^2 + s12.^2)); %angle from z axis

r2 = s20.*DOP2; %length of polarization vector from origin
theta2 = atan(s22./s21); %angle from x axis
phi2 = pi/2 - atan(s23./sqrt(s21.^2 + s22.^2)); %angle from z axis

%% Plot polarization angles over time and Poincare sphere projection

% Theta vs. time (in seconds)
figure(10)
plot(t2/1000,detrend(theta2),t1/1000,detrend(theta1))
xlabel('Time (s)','FontSize',12,'FontWeight','bold')
ylabel('Polarization Angle \theta (rad)','FontSize',12,'FontWeight','bold')
legend('SMF-28 Round Trip','Baseline')

% Phi vs. time
figure(20)
plot(t2/1000,detrend(phi2),t1/1000,detrend(phi1))
xlabel('Time (s)','FontSize',12,'FontWeight','bold')
ylabel('Polarization Angle \phi (rad)','FontSize',12,'FontWeight','bold')
legend('SMF-28 Round Trip','Baseline')

```

```
61
62 % Theta vs. Phi
63 figure(30)
64 plot(detrend(theta2),detrend(phi2),detrend(theta1),detrend(phi1))
65 ylabel('Polarization Angle \phi (rad)','FontSize',12,'FontWeight','bold')
66 xlabel('Polarization Angle \theta (rad)','FontSize',12,'FontWeight','bold')
67 legend('SMF-28 Round Trip','Baseline')
```

Bibliography

[ADM16] William M. Arkin, Ken Dilanian, and Cynthia McFadden. “What Obama Said to Putin on the Red Phone About the Election Hack”. In: *National Broadcasting Company News* (Dec. 19, 2016).

[Ame+16] American Civil Liberties Union et al. *Predictive Policing Today: A Shared Statement of Civil Rights Concerns*. The Leadership Conference on Civil and Human Rights, Aug. 31, 2016. http://civilrightsdocs.info/pdf/FINAL_JointStatementPredictivePolicing.pdf.

[Aru+19] Frank Arute et al. “Quantum supremacy using a programmable superconducting processor”. In: *Nature* (Oct. 23, 2019). DOI: 10.1038/s41586-019-1666-5.

[Bal18] Philip Ball. “Jian-Wei Pan: building the quantum internet”. In: *National Science Review* 6.2 (Sept. 21, 2018).

[BB14] Charles H Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *Theoretical Computer Science* 560 (Dec. 4, 2014), pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025.

[BB20] Chris Buckley and Keith Bradsher. “China Imposes Security Law on Hong Kong, Brushing Aside Opponents”. In: *The New York Times* (June 30, 2020).

[Bel64] John S Bell. “On the einstein podolsky rosen paradox”. In: *Physics Physique Fizika* 1.3 (Nov. 4, 1964), p. 195.

[Ben+96] Charles H. Bennett et al. “Mixed-state entanglement and quantum error correction”. In: *Physical Review A - Atomic, Molecular, and Optical Physics* 54.5 (Nov. 1, 1996), pp. 3824–3851. DOI: 10.1103/PhysRevA.54.3824.

[Ber+02] Steven Bernstein et al. “Glownet and Bossnet Gigabit Network Infrastructure for e-VLBI Glownet and Bossnet Multi-Gigabit / sec Optical Fiber Networks”. In: *Lincoln Laboratory eVLBI Workshop* April (Apr. 8, 2002), pp. 1–32.

[BL18] Erica Borghard and Shawn Lonergan. “Why Are There No Cyber Arms Control Agreements?” In: *Council on Foreign Relations* (Jan. 16, 2018).

[Blo+14] B. J. Bloom et al. “An optical lattice clock with accuracy and stability at the 10-18 level”. In: *Nature* 506.7486 (Jan. 22, 2014), pp. 71–75. DOI: 10.1038/nature12941.

[Bor+09] D. M. Boroson et al. “The Lunar Laser Communications Demonstration (LLCD)”. In: *Proceedings - 3rd IEEE International Conference on Space Mission Challenges for Information Technology*. Aug. 28, 2009, pp. 23–28. DOI: 10.1109/SMC-IT.2009.57.

[Bri10] Michael Bristow. “China defends internet censorship”. In: *British Broadcasting Corporation News* (June 8, 2010).

[BS20] Christopher Bing and Raphael Satter. “U.S. cybersecurity experts see recent spike in Chinese digital espionage”. In: *Reuters* (Mar. 25, 2020).

[Buc17] Ben Buchanan. *The cybersecurity dilemma: Hacking, trust, and fear between nations*. 1st ed. Oxford University Press, 2017. DOI: 10.1093/acprof:oso/9780190665012.001.0001.

[Bun+18] Darius Bunandar et al. “Metropolitan Quantum Key Distribution with Silicon Photonics”. In: *Physical Review X* 8.2 (Apr. 6, 2018), p. 021009. DOI: 10.1103/PhysRevX.8.021009.

[Cal+14] D. Calonico et al. “High-accuracy coherent optical frequency transfer over a doubled 642-km fiber link”. In: *Applied Physics B: Lasers and Optics* 117.3 (Sept. 4, 2014), pp. 979–986. DOI: 10.1007/s00340-014-5917-8.

[Cal+18] S. A. Caldwell et al. “Parametrically Activated Entangling Gates Using Transmon Qubits”. In: *Phys. Rev. Applied* 10.3 (Sept. 24, 2018), p. 034050. DOI: 10.1103/PhysRevApplied.10.034050.

[CB95] Clayton Christensen and J. L. Bower. “Disruptive technologies: catching the wave”. In: *Long Range Planning* 28.2 (Apr. 1995), p. 155. DOI: 10.1016/0024-6301(95)91075-1.

[Cha+09] T. E. Chapuran et al. “Optical networking for quantum key distribution and quantum communications”. In: *New Journal of Physics* 11 (Oct. 7, 2009). DOI: 10.1088/1367-2630/11/10/105001.

[Chi11] China Daily Editorial Board. "Cyber cooperation needed". In: *China Daily* (Nov. 22, 2011).

[Chu00] Isaac L. Chuang. "Quantum algorithm for distributed clock synchronization". In: *Physical Review Letters* 85.9 (Aug. 28, 2000), pp. 2006–2009. DOI: 10.1103/PhysRevLett.85.2006.

[Cli09] Hillary Rodham Clinton. *Closing Remarks for U.S.-China Strategic and Economic Dialogue*. July 28, 2009. Retrieved from https://web.archive.org/web/20090729230632/http://www.state.gov/secretary/rm/2009a/july/126599.htm.

[CNC19] CNCERT. *Summary of China's Internet Network Security Situation in 2019 (translated)*. Beijing, Apr. 2019. Retrieved from https://www.cert.org.cn/publish/main/upload/File/2019%20CNCERT%20Cybersecurity%20analysis.pdf.

[Com19] Combat Capabilities Development Command Army Research Laboratory Public Affairs. "Army project brings quantum internet closer to reality". In: *The United States Army Press* (Sept. 26, 2019).

[Cor+13] James C. Corbett et al. "Spanner: Google's Globally-Distributed Database". In: *ACM Transactions on Computer Systems* 31.3 (Aug. 2013). DOI: 10.1145/2491245.

[CR13] Kendall Card and Michael Rogers. *Navy Strategy for Achieving Information Dominance (2013-2017)*. U.S. Navy, 2013. https://www.public.navy.mil/fcc-c10f/Strategies/Navy_Strategy_for_Achieving_Information_Dominance.pdf.

[Cyb16] Cyber Administration of China. *National Cybersecurity Strategy*. Dec. 27, 2016. Retrieved from http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

[Dav19] Leonard David. "Farside Politics: The West Eyes Moon Cooperation with China". In: *Scientific American* (Feb. 7, 2019).

[Dea19] Dani Deahl. "Google employees demand the company pull out of Pentagon AI project". In: *The Verge* (Apr. 4, 2019).

[Dep08] Department of Treasury. *U.S.-China Strategic Economic Dialogue*. Dec. 2008. Retrieved from https://web.archive.org/web/20090617100850/http://www.ustreas.gov/initiatives/us-china/.

[Dep14] Department of Justice. *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*. May 19, 2014. Retrieved from https://www.justice.gov/opa/pr/us-

charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[Dep16] Department of Justice. *Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information*. Mar. 23, 2016. Retrieved from https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive.

[Dep17a] Department of Commerce. *Joint Release: Initial Results of the 100-Day Action Plan of the U.S.-China Comprehensive Economic Dialogue*. May 11, 2017. Retrieved from https://www.commerce.gov/news/press-releases/2017/05/joint-release-initial-results-100-day-action-plan-us-china-comprehensive.

[Dep17b] Department of Justice. *U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage*. Nov. 27, 2017. Retrieved from https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

[Dep18a] Department of Justice. *Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies*. Oct. 10, 2018. Retrieved from https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading.

[Dep18b] Department of Justice. *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*. Dec. 20, 2018. Retrieved from https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[Dep19] Department of Justice. *Member of Sophisticated China-Based Hacking Group Indicted for Series of Computer Intrusions, Including 2015 Data Breach of Health Insurer Anthem Inc. Affecting Over 78 Million People*. May 9, 2019. Retrieved from https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including.

[Dep20a] Department of Justice. *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency*

Equifax. Feb. 10, 2020. Retrieved from https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

[Dep20b] Department of Justice. *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research*. July 21, 2020. Retrieved from https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

[Dep20c] Department of State. *China Archives*. July 2020. Retrieved from https://www.state.gov/countries-areas-archive/china/page/2/.

[Dep20d] Department of Treasury. *U.S.-China Comprehensive Economic Dialogue*. July 2020. Retrieved from https://www.treasury.gov/initiatives/Pages/china.aspx.

[DH76] Whitfield Diffie and Martin E. Hellman. "New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22 (Nov. 1976). DOI: 10.1109/TIT.1976.1055638.

[Doe09] Sheperd Doeleman. "High frequency very long baseline interferometry: Frequency standards and imaging an event horizon". In: *Proceedings of the 7th Symposium on Frequency Standards and Metrology, ISFSM*. 2009, pp. 175–183. DOI: 10.1142/9789812838223_0018.

[Dro+14] Stefan Droste et al. "Optical frequency transfer over a single-span 1840-km fiber link". In: *2013 Joint European Frequency and Time Forum and International Frequency Control Symposium, EFTF/IFC 2013*. Jan. 9, 2014, pp. 1004–1006. DOI: 10.1109/EFTF-IFC.2013.6702150.

[Eke91] Artur K Ekert. "Quantum Cryptography Based on Bell's Theorem". In: *Physical Review Letters* (Aug. 5, 1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661.

[Eur16] European Space Agency. *ESA's Dragon cooperation with China extended to 2020*. Aug. 2016. Retrieved from https://www.esa.int/Applications/Observing_the_Earth/ESA_s_Dragon_cooperation_with_China_extended_to_2020.

[Eur19] European Space Agency. *ESA and NASA to team up on lunar science*. Mar. 28, 2019. Retrieved from https://www.esa.int/Science_Exploration/Human_and_Robotic_Exploration/Exploration/ESA_and_NASA_to_team_up_on_lunar_science.

[FC20] Emily Feng and Amy Cheng. “Chinese Universities Are Enshrining Communist Party Control In Their Charters”. In: *National Public Radio* (Jan. 20, 2020).

[Fig18] Patricia Figliola. *Federal Quantum Information Science: An Overview*. Congressional Research Service, July 2, 2018. https://fas.org/sgp/crs/misc/IF10872.pdf.

[Fig19] Patricia Figliola. *Quantum Information Science: Applications, Global Research and Development, and Policy Considerations*. Congressional Research Service, Nov. 1, 2019. https://crsreports.congress.gov/product/pdf/R/R45409.

[Fio16] Daniel Fiott. “Europe and the Pentagon’s Third Offset Strategy”. In: *The RUSI Journal* 161.1 (Mar. 11, 2016), pp. 26–31. DOI: 10.1080/03071847.2016.1152118.

[Get20] Jeffrey Gettleman. “In Ladakh, Caught Between the Troops of India and China”. In: *The New York Times* (July 11, 2020).

[GJC12] Daniel Gottesman, Thomas Jennewein, and Sarah Croke. “Longer-baseline telescopes using quantum repeaters”. In: *Physical Review Letters* 109.7 (Aug. 16, 2012). DOI: 10.1103/PhysRevLett.109.070503.

[Gre+17] Matthew E. Grein et al. “Stabilization of long, deployed optical fiber links for quantum networks”. In: *Conference on Lasers and Electro-Optics Proceedings*. May 2017. DOI: 10.1364/CLEO_QELS.2017.FTu4F.6.

[Gre05] Susan Greenhalgh. “Missile science, population science: The origins of China’s one-child policy”. In: *China Quarterly* 53.182 (June 2005), pp. 253–276. DOI: 10.1017/S0305741005000184.

[Gre16] Kieran Green. “People’s War in Cyberspace: Using China’s Civilian Economy in the Information Domain”. In: *Military Cyber Affairs* 2.1 (Dec. 2016). DOI: 10.5038/2378-0789.2.1.1022.

[Gui14] Gwynn Guilford. “The world leader in bike-sharing is… China”. In: *Quartz* (Aug. 25, 2014).

[GW18] Jack Goldsmith and Robert Williams. “The Failure of the United States’ Chinese-Hacking Indictment Strategy”. In: *Lawfare* (Dec. 28, 2018).

[Hal+07] Matthäus Halder et al. “Entangling independent photons by time measurement”. In: *Nature Physics* 3.10 (Aug. 19, 2007), pp. 692–695. DOI: 10.1038/nphys700.

[He19] Laura He. “China just signaled that it could reform its IP laws. That’s good for trade talks”. In: *Cable News Network* (Nov. 25, 2019).

[Hod19] Rae Hodge. "US Army bans TikTok app from government phones". In: *CNET* (Dec. 31, 2019).

[Hol20] Steve Holland. "U.S., China agree to semi-annual talks aimed at reforms, resolving disputes". In: *Reuters* (Jan. 11, 2020).

[IBM20] IBM Q. *Quantum Computing at IBM*. July 2020. Retrieved from https://www.ibm.com/quantum-computing/learn/what-is-ibm-q/.

[Int16] FireEye iSIGHT Intelligence. *Redline Drawn: China Recalculates Its Use of Cyber Espionage*. FireEye, 2016. https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

[Joz+00] Richard Jozsa et al. "Quantum clock synchronization based on shared prior entanglement". In: *Physical Review Letters* 85.9 (Aug. 28, 2000), pp. 2010–2013. DOI: 10.1103/PhysRevLett.85.2010.

[Kal19] Kali Linux. *Penetration Testing and Ethical Hacking Linux Distribution*. July 2019. Retrieved from https://www.kali.org/.

[KC18] Elsa B Kania and John K Costello. *Quantum Hegemony?* Center for New American Security, Sept. 12, 2018. https://www.cnas.org/publications/reports/quantum-hegemony.

[Kea20] Sean Keane. "Huawei ban: Full timeline as it posts smallest profit increase in 3 years". In: *CNET* (July 22, 2020).

[Kem14] R Scott Kemp. "The Nonproliferation Emperor Has No Clothes: The Gas Centrifuge, Supply-Side Controls, and the Future of Nuclear Proliferation". In: *International Security* 38.4 (May 28, 2014). DOI: 10.1162/ISEC_a_00159.

[KG20] Angus King and Mike Gallagher. *Cyberspace Solarium Commission*. Mar. 2020. https://www.solarium.gov/report.

[Kha+19a] E. T. Khabiboulline et al. "Optical Interferometry with Quantum Networks". In: *Physical Review Letters* 123.7 (Aug. 15, 2019), p. 070504. DOI: 10.1103/PhysRevLett.123.070504.

[Kha+19b] E. T. Khabiboulline et al. "Quantum-assisted telescope arrays". In: *Physical Review A* 100.2 (Aug. 15, 2019). DOI: 10.1103/PhysRevA.100.022316.

[Kim08] H. J. Kimble. "The quantum internet". In: *Nature* 453.7198 (June 18, 2008). DOI: 10.1038/nature07127.

[Kle+20] Kerstin Kleese van Dam et al. "From Long-distance Entanglement to Building a Nationwide Quantum Internet: Report of the DOE Quantum Internet Blueprint

Workshop". In: *Office of Scientific and Technical Information* (Feb. 5, 2020). DOI: 10.2172/1638794.

[KMW02] D. Kielpinski, C. Monroe, and D. J. Wineland. "Architecture for a large-scale ion-trap quantum computer". In: *Nature* 417.6890 (June 13, 2002), pp. 709–711. DOI: 10.1038/nature00784.

[Kóm+14] P. Kómár et al. "A quantum network of clocks". In: *Nature Physics* 10.8 (June 15, 2014), pp. 582–587. DOI: 10.1038/nphys3000.

[Kra19] Olga Krasnyak. "How U.S.-Soviet Scientific and Technical Exchanges Helped End the Cold War". In: *American Diplomacy* (Nov. 2019).

[Las18] Lorand Laskai. "Civil-Military Fusion: The Missing Link Between China's Technological and Military Rise". In: *Council on Foreign Relations* (Jan. 29, 2018).

[Led+17] Heidi Ledford et al. "Nature's 10". In: *Nature* 552.7685 (Dec. 2017), pp. 315–324. DOI: 10.1038/d41586-017-07763-y.

[Lee+18] Catherine Lee et al. "High-dimensional entanglement distribution and Einstein-Podolsky-Rosen steering over deployed fiber". In: *Conference on Lasers and Electro-Optics*. May 2018. DOI: 10.1364/CLEO_QELS.2018.FW4F.4.

[Leo19] Jenny Leonard. "China's Thousand Talents Program Finally Gets the U.S.'s Attention". In: *Bloomberg* (Dec. 12, 2019).

[Li03] Cheng Li. "Educational and professional backgrounds of current provincial leaders". In: *China Leadership Monitor* 8 (Oct. 2003).

[Li20] Pei Li. "Tencent to invest $70 billion in 'new infrastructure'". In: *Reuters* (May 26, 2020).

[Lia+17] Sheng Kai Liao et al. "Satellite-to-ground quantum key distribution". In: *Nature* 549.7670 (Aug. 9, 2017), pp. 43–47. DOI: 10.1038/nature23655.

[Loc90] John Locke. *Two Treatises of Government*. 10th ed. Project Gutenberg, 1690.

[Lom+16] Michael A Lombardi et al. "Accurate, Traceable, and Verifiable Time Synchronization for World Financial Markets". In: *Journal of Research of the National Institute of Standards and Technology* 121 (Oct. 7, 2016). DOI: 10.6028/jres.121.023.

[Lor13] Peter Lorentzen. "China's Strategic Censorship". In: *American Journal of Political Science* 58.2 (Oct. 8, 2013), pp. 402–414. DOI: 10.1111/ajps.12065.

[LX95] John Lewis and Litai Xue. "China's Strategic Seapower: The Politics of Force Modernization in the Nuclear Age". In: *The China Quarterly* 144 (Dec. 1995), pp. 1207–1209. DOI: 10.1017/s030574100000494x.

[Mai20] Lindsay Maizland. "China's Repression of Uighurs in Xinjiang". In: *Council on Foreign Relations* (June 30, 2020).

[Mal18] Smriti Mallapaty. "Paper authorship goes hyper". In: *Nature Index* (Jan. 30, 2018).

[Man13] Mandiant. *APT1: Exposing One of China's Cyber Espionage Units*. FireEye, 2013. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[Man18] Jennifer Manning. *Membership of the 115th Congress: A Profile*. Congressional Research Service, Dec. 20, 2018. https://fas.org/sgp/crs/misc/R44762.pdf.

[MD18] Anna Mitchell and Larry Diamond. "China's Surveillance State Should Scare Everyone". In: *The Atlantic* (Feb. 2, 2018).

[Mer78] Ralph C. Merkle. "Secure Communications Over Insecure Channels". In: *Communications of the ACM* (Apr. 1978). DOI: 10.1145/359460.359473.

[MGB20] Willem Marx, David Gura, and Eric Baculinao. "Coronavirus: As pandemic worsens so do U.S.-China relations". In: *National Broadcasting Company News* (Mar. 18, 2020).

[Moz15] Paul Mozur. "Baidu and CloudFlare Boost Users Over China's Great Firewall". In: *The New York Times* (Sept. 13, 2015).

[MS20] David McCabe and Ana Swanson. "Trump Effort to Keep U.S. Tech Out of China Alarms American Firms". In: *The New York Times* (Feb. 16, 2020).

[Mun+15] William J. Munro et al. "Inside Quantum Repeaters". In: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (Jan. 15, 2015), pp. 78–90. DOI: 10.1109/JSTQE.2015.2392076.

[Nak18] Paul M. Nakasone. *Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. Cyber Command*. Apr. 2018, pp. 1–12. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information*. 10th ed. Cambridge: Cambridge University Press, 2010, p. 702. DOI: 10.1017/CBO9780511976667.

[NCS20] NCSC. *Quantum security technologies*. Mar. 24, 2020, pp. 1–4. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.

[NR18] Deborah J. Nightingale and Donna H. Rhodes. *Architecting the Future Enterprise*. Cambridge: The MIT Press, 2018. DOI: 10.7551/mitpress/9290.001.0001.

[NW12] Ellen Nakashima and Joby Warrick. "Stuxnet was work of U.S. and Israeli experts, officials say". In: *The Washington Post* (June 2, 2012).

[Nye08] Joseph S. Nye. "Public diplomacy and soft power". In: *Annals of the American Academy of Political and Social Science* (Mar. 1, 2008). DOI: 10.1177/0002716207311699.

[Off13] Office of the Press Secretary. *FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security*. June 17, 2013. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

[Off15] Office of the Press Secretary. *FACT SHEET: President Xi Jinping's State Visit to the United States*. Sept. 25, 2015. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[Off19] Office of the Historian. *Milestones: 1969–1976*. 2019. Retrieved from https://history.state.gov/milestones/1969-1976/salt.

[Off20a] Office of Naval Research. *Programs - Quantum Information Science*. 2020. Retrieved from https://www.onr.navy.mil/en/Science-Technology/Departments/Code-31/All-Programs/312-Electronics-Sensors/quantum-information-science.

[Off20b] Office of the Spokesperson. *Briefing With Senior State Department Officials on China's Expulsion of U.S. Journalists*. Mar. 18, 2020. Retrieved from https://www.state.gov/briefing-with-senior-state-department-officials-on-chinas-expulsion-of-u-s-journalists/.

[Off67] Office of the State Department. *Outer Space Treaty*. Oct. 10, 1967. Retrieved from https://2009-2017.state.gov/t/isn/5181.htm.

[Ost15] Elinor Ostrom. *Governing the commons: The evolution of institutions for collective action*. Cambridge: Cambridge University Press, 2015. DOI: 10.1017/CBO9781316423936.

[Pag19] Jeremy Page. "America's Undersea Battle With China for Control of the Global Internet Grid". In: *Wall Street Journal* (Mar. 12, 2019).

[Pet+09] N A Peters et al. “Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments”. In: *New Journal of Physics* 11.4 (Apr. 30, 2009). DOI: 10.1088/1367-2630/11/4/045012.

[Pin+20] J. M. Pino et al. “Demonstration of the QCCD trapped-ion quantum computer architecture”. In: *arXiv preprint arXiv:2003.01293* (Mar. 3, 2020).

[Pom20a] Michael Pompeo. *A New Transatlantic Dialogue*. Washington, D.C. German Marshall’s Brussels Forum, June 25, 2020. Retrieved from https://www.state.gov/a-new-transatlantic-dialogue/.

[Pom20b] Michael Pompeo. *Silicon Valley and National Security*. San Francisco. Commonwealth Club, Jan. 13, 2020. Retrieved from https://www.state.gov/silicon-valley-and-national-security/.

[Pre98] John Preskill. “Reliable quantum computers”. In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 454.1969 (Jan. 8, 1998), pp. 385–410. DOI: 10.1098/rspa.1998.0167.

[PS18] Nicole Perlroth and David E. Sanger. “Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says”. In: *The New York Times* (Mar. 15, 2018).

[Rai18] Lee Rainie. “How Americans feel about social media and privacy”. In: *Pew Research Center* (Mar. 27, 2018).

[RB14] Thomas Rid and Ben Buchanan. “Attributing Cyber Attacks”. In: *Journal of Strategic Studies* 38.1-2 (Dec. 23, 2014), pp. 4–37. DOI: 10.1080/01402390.2014.977382.

[Ric14] Steven Rich. “NSA seeks to build quantum computer that could crack most types of encryption”. In: *The Washington Post* (Jan. 2, 2014).

[RM19] Eric Rosenbach and Katherine Mansted. “The Geopolitics of Information”. In: *Belfer Center for Science and International Affairs* (May 28, 2019).

[Rob20] Adi Robertson. “Congress introduces EARN IT Act limiting websites’ Section 230 shield”. In: *The Verge* (Mar. 5, 2020).

[RS19] Michael Raggi and Dennis Schwarz. *LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards*. Proofpoint, Aug. 1, 2019. https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks.

[RSA78] Ronald Rivest, Adi Shamir, and Leonard Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Communications of the ACM* 21.2 (Feb. 1978). DOI: 10.1145/359340.359342.

[San20] David Sanger. "Grindr Is Owned by a Chinese Firm, and the U.S. Is Trying to Force It to Sell". In: *The New York Times* (Mar. 28, 2020).

[Sat19] Adam Satariano. "How the Internet Travels Across Oceans". In: *The New York Times* (Mar. 10, 2019).

[SB15] Richard Spencer and David Blair. "MIT, a whiteboard and nuclear physics: how the Iran deal was struck". In: *The Telegraph* (Apr. 4, 2015).

[Sco18] Kevin Scott. *Joint Doctrine Note 1-18*. Department of Defense, Apr. 25, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_18.pdf?ver=2018-04-25-150439-540.

[SCW17] Lamar Smith, Barbara Comstock, and Randy Weber. *Joint Hearing on American Leadership in Quantum Technology*. Oct. 24, 2017. Retrieved from https://www.govinfo.gov/content/pkg/CHRG-115hhrg27671/html/CHRG-115hhrg27671.htm.

[SE08] Roald Sagdeev and Susan Eisenhower. "United States-Soviet Space Cooperation during the Cold War". In: *NASA 50th Anniversary Magazine* (July 2008).

[Sho97] Peter W. Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509. DOI: 10.1137/S0097539795293172.

[Sin00] Simon Singh. *The Code Book: The Science of Secrecy from Ancient Egypt To Quantum Cryptography*. 2nd ed. New York: Anchor Books, 2000.

[SP19] David E. Sanger and Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power Grid". In: *The New York Times* (June 15, 2019).

[Ste15] Phil Stewart. "U.S., China agree on rules for air-to-air military encounters". In: *Reuters* (Sept. 25, 2015).

[Ste16] Mark Stevens. "Fiber Delay Analysis and Control Loop Design for Quantum Illumination". In: *MIT Lincoln Laboratory Group 67 Internal Memorandum* (Feb. 10, 2016).

[Sti19] David Stilwell. *U.S.-China Bilateral Relations: The Lessons of History*. Washington, D.C. Center for Strategic and International Studies, Dec. 12, 2019. Retrieved from

https://www.state.gov/u-s-china-bilateral-relations-the-lessons-of-history/.

[Sun18] Yiting Sun. "Why Alibaba is betting big on AI chips and quantum computing". In: *MIT Technology Review* (Sept. 25, 2018).

[Swa19] Michael Swaine. "A Relationship Under Extreme Duress: U.S.-China Relations at a Crossroads". In: *Carnegie Endowment for International Peace* (Jan. 16, 2019).

[Tap+05] B Tapley et al. "GGM02 - An improved Earth gravity field model from GRACE". In: *Journal of Geodesy* 79.8 (Sept. 16, 2005), pp. 467–478. DOI: 10.1007/s00190-005-0480-z.

[Tea19] Crowdstrike Global Intelligence Team. *Global Threat Report: Adversary Tradecraft and the Importance of Speed*. 2019. https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/.

[Toc40] Alexis de Tocqueville. *Democracy in America*. 1st ed. Chicago: University of Chicago Press, 1840. DOI: 10.5840/thought194520396.

[Tre+19] Christoph Tresp et al. "Characterization of the CEO phase noise of an erbium fiber frequency comb". In: *Conference on Lasers and Electro-Optics*. May 2019. DOI: 10.1364/CLEO_SI.2019.STu4L.4.

[Vol18] Dustin Volz. "FBI chief calls unbreakable encryption 'urgent public safety issue'". In: *Reuters* (Jan. 9, 2018).

[Wan10] Huiyao Wang. *China's National Talent Plan: Key Measures and Objectives*. Brookings Institute, Nov. 23, 2010. https://www.brookings.edu/research/chinas-national-talent-plan-key-measures-and-objectives/.

[WB20] Edward Wong and Julian E. Barnes. "U.S. to Expel Chinese Graduate Students With Ties to China's Military Schools". In: *The New York Times* (May 28, 2020).

[WEH18] Stephanie Wehner, David Elkouss, and Ronald Hanson. "Quantum internet: A vision for the road ahead". In: *Science* 362.6412 (Oct. 19, 2018). DOI: 10.1126/science.aam9288.

[Whe20] Mike Wheatley. "Baidu open-sources its Paddle Quantum machine learning toolkit on GitHub". In: *SiliconANGLE* (May 28, 2020).

[Whi18] White House. *National Cyber Strategy of the United States of America*. Sept. 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[Whi20] White House. *Executive Order on Securing the United States Bulk-Power System*. May 1, 2020. https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/.

[WL18] John Walcott and Jonathan Landay. "Russian spy chief met U.S. officials in U.S. last week: sources". In: *Reuters* (Jan. 30, 2018).

[Woo19] Chris Woolston. "US-China science weathers political ill wind". In: *Nature* 575.7783 (Nov. 20, 2019), S26–S27. DOI: 10.1038/d41586-019-03541-0.

[WP18] Greg Walden and Frank Pallone. *Hearing on Disrupter Series: Quantum Computing*. May 18, 2018. Retrieved from https://energycommerce.house.gov/committee-activity/hearings/hearing-on-disrupter-series-quantum-computing-subcommittee-on-digital.

[Yin19] Fu Ying. "Communication Means Dialogue Among People". In: *China US Focus* (Aug. 19, 2019).

[Yun18] Man-Hong Yung. *Going beyond Moore's Law with quantum computing*. Dec. 28, 2018. Retrieved from https://www.huawei.com/us/publications/communicate/86/quantum-computing-ai.

[Zha+18] Helena Zhang et al. "Measurement of Fiber-Induced One-Way Noise over Deployed Optical Links for Quantum Networks". In: *IEEE Photonics Society Summer Topicals Meeting Series, SUM 2018*. Institute of Electrical and Electronics Engineers Inc., Sept. 6, 2018, pp. 75–76. DOI: 10.1109/PHOSST.2018.8456710.

[Zha+19] Qiang Zhang et al. "Quantum information research in China". In: *Quantum Science and Technology* 4.4 (Nov. 8, 2019). DOI: 10.1088/2058-9565/ab4bea.

[Zha19] Helena Zhang. "Toward a Quantum Clock Network". Doctoral dissertation. Massachusetts Institute of Technology (Department of Physics), 2019.

[Zho17] Viola Zhou. "Out with the technocrats, in with China's new breed of politicians". In: *South China Morning Post* (Oct. 26, 2017).

[Zim96] Philip Zimmerman. *PGP User's Guide*. 1st ed. Cambridge: The MIT Press, 1996.

[ZL20] Josh Zumbrun and Catherine Lucey. "Trump Dims Hopes for New China Trade Deal". In: *The Wall Street Journal* (July 10, 2020).